| 文書管理番号 | 技開 18-003 |
|---|---|

# PostgreSQL 認証版

# セキュリティターゲット

1.0版

発行日： 2007/3/9

株式会社NTTデータ

| 保管期間 | 次期改版時 |
|---|---|

| 全ページ数 | 100 ページ |
|---|---|

# 更新履歴表

| 文書名 ： PostgreSQL 認証版 セキュリティターゲット | | | | 文書管理番号：<br>技開 18-003 | |
|---|---|---|---|---|---|
| 版数 | 更新日 | 更新個所 | 更新内容（概要） | 更新者 | 承認者 |
| 1.0 | 2007/03/09 | 初版 | | 政谷 K | 田中 B |
| | | | | | |

# まえがき

## 本書の目的

本書は，ISO/IEC15408 に基づいた「PostgreSQL 認証版」のセキュリティターゲットである。

## 本書の構成

本書は，以下のように構成している.

１章　ST 概説：本セキュリティターゲットについて概説している。

２章　TOE 記述：製品についての概説を記述している。

３章　TOE セキュリティ環境：製品が使われると想定する環境のセキュリティの側面について記述している。

４章　セキュリティ対策方針：TOE およびその環境に対するセキュリティ対策方針について記述している。

５章　ＩＴセキュリティ要件：TOE またはその環境が満たすＩＴセキュリティ要件を詳細に定義している。

６章　TOE 要約仕様：TOE に対するセキュリティ要件を具体的に定義している。

７章　PP 主張：PP の準拠性について記述している。

８章　根拠：TOE セキュリティ環境において識別されたすべての側面を追跡することができ、かつそれらをカバーするのに適していることを実証している。

## 商標

# 目次

## 表目次



## 図目次

# 1. ST 概説

セキュリティターゲットの概要を述べる。

## 1.1. ST 識別

### 1.1.1. ST 識別

名称： 「PostgreSQL 認証版 セキュリティターゲット」
版番号： 1.0 版
作成者名： 株式会社ＮＴＴデータ
作成日： 2007/3/9
適用する CC バージョン： CC v2.3 （補足-0512 適用）

### 1.1.2. TOE 識別

TOE 名: PostgreSQL 認証版
版番号: Linux 版 V8.1.5
製作者: 株式会社ＮＴＴデータ

## 1.2. ST 概要

PostgreSQL 認証版 Linux 版 V8.1.5 (以後、PostgreSQL 認証版)はリレーショナルデータベース機能を提供するソフトウェア製品である。本「PostgreSQL 認証版セキュリティターゲット」は PostgreSQL 認証版を利用する上でのセキュリティ上の脅威を分析し､それらの脅威に対する対策として PostgreSQL 認証版が提供するセキュリティ機能について記述することにより、PostgreSQL 認証版の安全性および堅牢性を証明することを目的としている。

## 1.3. CC 適合

本 TOE の CC 適合は以下のとおりである。

適用する CC のバージョン： CC v2.3
補足-0512 適用

- 機能要件: CC パート 2 適合
- 保証要件:CC パート 3 適合
- 評価保証レベル EAL1 適合
- 適合する PP は存在しない

## 1.4. 参照資料

- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model August 2005 Version 2.3
  CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements August 2005 Version 2.3
  CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements August 2005 Version 2.3
  CCMB-2005-08-003
- 情報技術セキュリティ評価のためのコモンクライテリア
  パート 1：概説と一般モデル、2005 年 8 月、バージョン 2.3、CCMB-2005-08-001
  パート 2：セキュリティ機能要件、2005 年 8 月、バージョン 2.3、CCMB-2005-08-002
  パート 3：セキュリティ保証要件、2005 年 8 月、バージョン 2.3、CCMB-2005-08-003
  いずれも平成 17 年 12 月翻訳第 1.0 版　　独立行政法人情報処理推進機構セキュリティセンター
- 補足文書
  補足−0512

# 2. TOE 記述

本 TOE の概要、運用環境、機能概要について説明する。

## 2.1. TOE の種別と製品構成

本 TOE はリレーショナルデータベース機能を提供するソフトウェア製品である。
本 TOE 製品、PostgreSQL 認証版は、Red Hat Enterprise Linux AS v.4 for x86 OS の動作するサーバ上に導入されるソフトウェアパッケージであり、下表に示す単一のパッケージから構成される。パッケージはインストールすることによって、標準で TOE の機能を利用できるように構成してある。

**表 2.1 PostgreSQL 認証版の製品構成**

| 項番 | パッケージ名 | バージョン | 機能 |
|---|---|---|---|
| 1 | postgresql-iso15408-8.1.5 | Linux 版<br>V8.1.5 | RDB サーバ機能<br>PostgreSQL 関連コマンド |

## 2.2. TOE の動作環境

本TOEの動作環境を「図 2.1　TOEの動作環境」に示す。本TOEは Intel Architecture に準拠したマイクロプロセッサを搭載した単一のサーバマシン上で動作する。サーバマシンおよびそのコンソールは物理的に保護されたセキュリティ専用区域に設置される。セキュリティ専用区域への入室権限はシステムおよびサーバの運用管理者が持つ。
サーバが接続されるネットワークはファイアウォールによって保護されたセキュアなＬＡＮである。ファイアウォールは特定のポートに対する特定の端末からのパケットだけが通過できるように設定され、当該のＬＡＮを保護する。

### 2.2.1. ハードウェア

本 TOE は Intel Architecture に準拠したマイクロプロセッサを搭載したサーバマシン上で動作する。
本 TOE はソフトウェア製品であり、ハードウェア構成は次節に示す OS が動作するもので必要十分であり、付加的な装置・機器を要するものではない。
サーバハードウェアの各リソースは以下の指標を満たすものとする。

- プロセッサ　400MHz 以上
- メモリ　1GB 以上
- ハードディスク　2GB 以上

### 2.2.2. ソフトウェア

本 TOE は「Red Hat Enterprise Linux AS v.4 for x86」上で動作する。
TOE は、本 OS と連携して、セキュリティ機能を提供する（OS は TOE の範囲外である）。

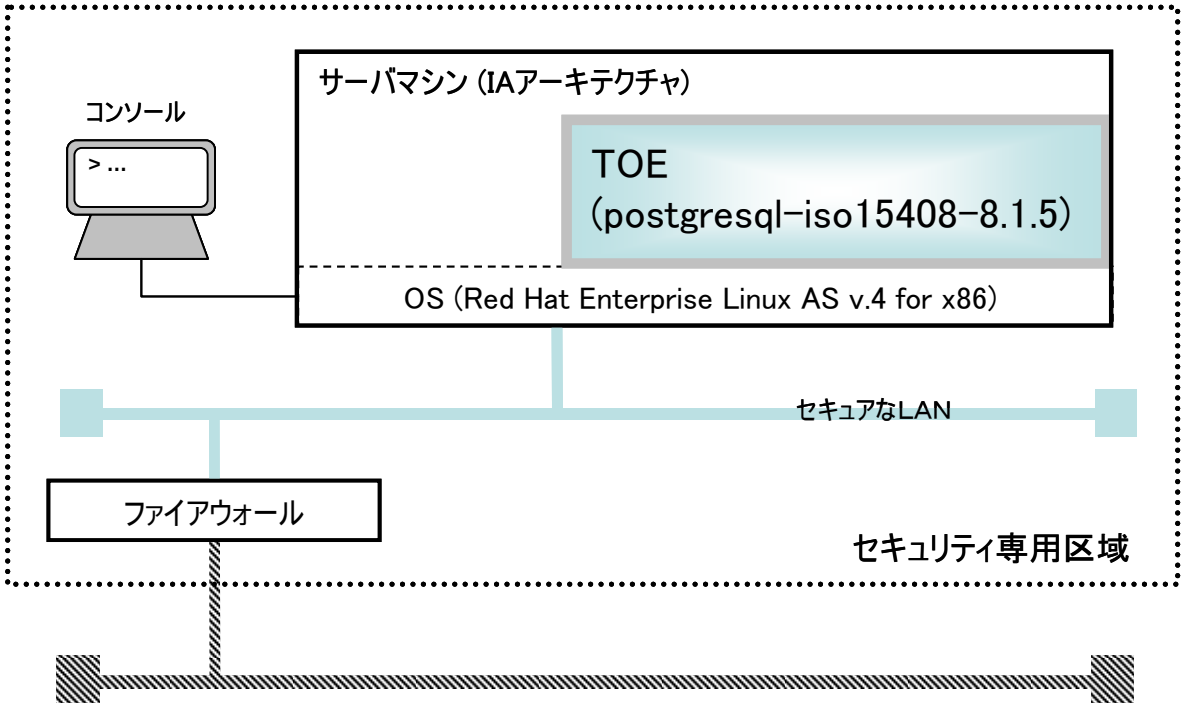


**図 2.1 TOE の動作環境**

## 2.3. TOE の利用

本 TOE の関係者と利用方法について説明する。

### 2.3.1. TOE の関係者

データベースの利用者にはデータ処理を目的に本 TOE を使用する一般利用者（以後、利用者）と、TOE の運用や管理業務を行う運用管理者（以後、管理者）が存在する。

#### 2.3.1.1. 利用者

利用者は、アプリケーションを使ってデータベースにアクセスする。
利用者がアプリケーションを使って TOE を利用するためには、TOE の利用を許可されている必要がある。TOE への利用許可は、管理者が TOE に利用者識別情報を登録することにより行われる。

#### 2.3.1.2. 管理者

管理者は、利用者の登録や、データベース用ファイル領域の設定など TOE の動作に必要な環境設定および、利用者の用いるアプリケーションのサーバ上への設置、ユーザ定義関数の登録などの管理業務を実施する。さらに、本 TOE を使ったシステムの運用環境を管理する（OS，ネットワーク，各種資源への

アクセス状況を監視し、バックアップ／リカバリなど必要な管理業務を行う)。
管理者は、OS の管理者でもある（以下、特に断らない限り、管理者とは TOE と OS の両方の管理者である)。
なお、管理者は、利用者が行える作業は全て行える。

#### 2.3.1.3. 責任者

責任者は、セキュリティシステムの全責任を担う責任者を指す。責任者は、ふさわしい管理者の選任、管理者の教育等を行う必要がある。

### 2.3.2. 利用方法

TOE の機能を利用するには、「OS にログインし、自システムで PostgreSQL 関連コマンドを通じて利用する方法」、「自システム上のアプリケーションが UNIX ドメインソケットを経由して利用する方法」、「他システム上のアプリケーションが TCP/IP ソケットを経由して利用する方法」の３つの方法が可能である。これらのうち TCP/IP ソケットを経由して利用する機能は、本 ST の運用環境では動作させないため、TOE の対象外とする。
本 ST の運用環境では、OS にログインし PostgreSQL **関連コマンド**を通じて TOE を利用する方法は管理者に限定される。即ち、管理者はローカルログインおよびネットワーク経由のログインを行なうことが可能であるが、利用者は OS にログインすることはできない。
利用者は常にシステム上のアプリケーションを経由して TOE を利用する。アプリケーションは OS の機能を用いてなんらかのインターフェースを利用者に提供するが、当該のアプリケーションおよびアプリケーションの提供するインターフェースは TOE の対象外である。

本 ST の運用環境では管理者および利用者は TOE の機能を、以下の方法で利用できる。

- 管理者が OS にログインした後に、自システム上で PostgreSQL 関連コマンドを実行し TOE の機能を利用する
- 自システム上で動作するアプリケーションが UNIX ドメインソケットを用いて TOE に接続し、SQL 言語を用いて TOE の機能を利用する。アプリケーションが TOE に接続する際、アプリケーションは TOE に登録された利用者（ないし管理者）の識別情報を提示する必要がある。

本 ST の運用環境では、他システムから TCP/IP ソケットを経由して TOE を利用する機能は動作させないため、TOE を直接リモートから利用することはできない。リモートからの利用は常にアプリケーションを介した間接的なものに限られる。その際のアプリケーションと TOE のインターフェースは上述の UNIX ドメインソケットを用いた接続に限定される (アプリケーションと TOE のインターフェースの限定は OS の機能を用いて実現される)。
本 ST の運用環境では利用者（ないし管理者）の識別をパスワード認証方式で行なうものとする。

## 2.4. TOE の構成と機能

TOE の構成と機能について説明する。

### 2.4.1. TOE の範囲

「図 2.2 TOEの論理構成」に本TOEの論理構成を示す。図中、灰色太線で囲まれた部分がTOEの範囲である。

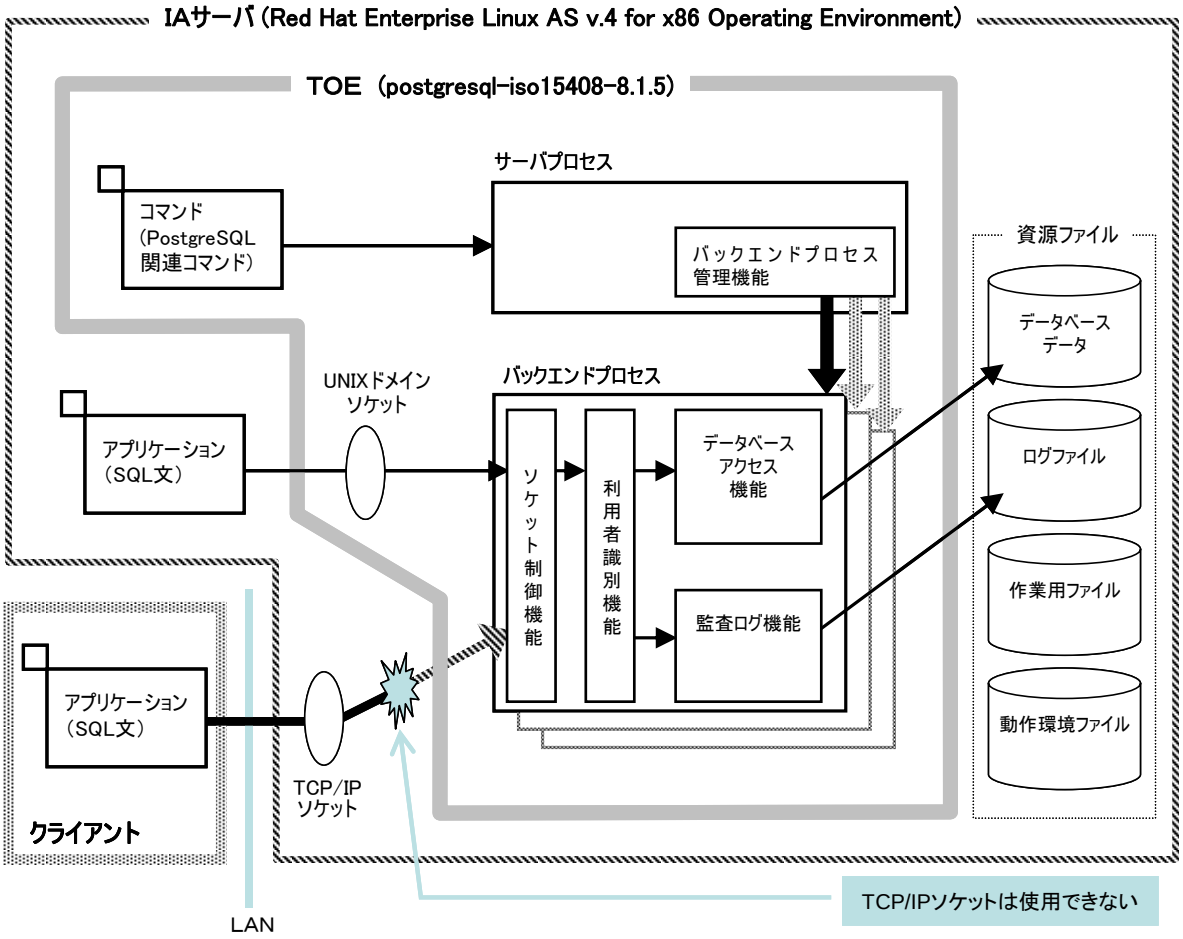


**図 2.2 TOE の論理構成**

管理者は PostgreSQL **関連コマンド**の実行を通して TOE を起動、停止する。PostgreSQL **関連コマンド**は TOE の範囲である（以降、コマンドと略記した場合は PostgreSQL 関連コマンドを意味する）。

TOE のリレーショナルデータベース機能を利用する場合、利用者および管理者は、アプリケーションを介して TOE に接続する。アプリケーションから TOE に接続する場合には、アプリケーションは TOE に対して利用者ないし管理者の識別情報を指定しパスワード認証を経た後に、SQL 文の処理を依頼する。アプリケーションの指定する識別情報に関連付けられた権限に従って、TOE はアプリケーションに埋め込まれた SQL 文を処理する。

アプリケーションから TOE への接続には UNIX ドメインソケットを経由する。TCP/IP ソケットを経由して接続する機能は本 ST 標準のセキュリティ運用では利用しないため TOE の対象外とする。また、識別はパスワード認証方式のみを用いる。

### 2.4.2. TOE の機能

本 TOE は以下の 5 つの機能を提供し、リレーショナルデータベース機能を実現している。

- バックエンドプロセス管理機能
- ソケット制御機能
- 利用者識別機能
- データベースアクセス機能
- 監査ログ機能

#### ■ バックエンドプロセス管理機能

サーバプロセスがバックエンドプロセスの起動、停止およびバックエンドプロセスとアプリケーションの接続を管理する機能である。本TOEでは、サーバプロセスはコマンドによって起動されTOE全体で一つである。一方バックエンドプロセスは、アプリケーションの処理に対応してサーバプロセスの子プロセスとして起動（図 2.2の上から下への太矢印)、管理される。バックエンドプロセスがマルチプロセス動作することで、利用者はアプリケーションを複数同時に実行する、あるいはひとつのアプリケーションの中で複数同時にSQL文の処理を依頼することができる。

#### ■ ソケット制御機能

サーバプロセスがアプリケーションから接続の要求を受けると、バックエンドプロセスに対して UNIX ドメインソケットを OS の管理機能を用いて割り付ける。バックエンドプロセスは UNIX ドメインソケット経由でアプリケーションと接続される。
管理者は、ソケット制御機能を用いてサーバプロセスが割り付けるソケットの種類や利用の可否、またソケットの接続数を制御することができる。

#### ■ 利用者識別機能

アプリケーションとバックエンドプロセスの接続において、各利用者の権限を制御し、指定された権限の範囲での処理を保証し、またその範囲を超えた処理を制限する機能である。バックエンドプロセスに接続されたアプリケーションが指定する識別情報を認証し、個々のバックエンドプロセスに論理的なアクセス権限を付与する。利用者の識別情報を指定して実行したバックエンドプロセスを利用者のプロセスと呼ぶ。また、管理者の識別情報を指定して実行したバックエンドプロセスを管理者のプロセスと呼ぶ。管理者が実行したコマンドのプロセスも管理者のプロセスである。

#### ■ データベースアクセス機能

利用者識別機能が関連付けた論理アクセス権限に従って、バックエンドプロセスが各利用者（ないし管理者）のデータおよびデータの構造定義情報の参照、更新等行なう機能である。データベースアクセス機能は、利用者識別機能が関連付けた論理的アクセス権限に従い、各利用者のデータおよびデータの構造定義情報を、当該の利用者のみが利用できることを保障する。

TOEは、リレーショナルデータベース機能で扱うデータを、ＯＳがTOEに割り当てる資源ファイル（参照：「2.5 TOEの利用する資源ファイルと保護資産」）に格納する。資源ファイルに格納されているデータに対して物理的なアクセスを行うのは、TOEのコマンドのプロセスとバックエンドプロセスである。バックエンドプロセスの資源ファイルへの物理的なアクセスは、TOEの管理者権限で行われるが、利用者データへの論理的なアクセスは、アプリケーションがTOEへの接続の際に指定した識別情報に利用者識別機能が関連付けた論理的アクセス権限に従って適切に制御される。従って、利用者のプロセスは当該の利用者のデータだけを利用できる。
また、バックエンドプロセスと資源ファイルは OS の機能を用いてアプリケーションから分離されているため、例えアプリケーションに論理ミス等があったとしても、アプリケーションが各利用者のデータや資源ファイルに、バックエンドプロセスを介さずに、直接アクセスすることはできない。

TOE が OS から獲得する資源ファイルおよびプロセス、UNIX ドメインソケットの保護は OS が行う。

データベースアクセス機能を利用するために、管理者および利用者は SQL 文を埋め込んだアプリケーションを通じて TOE に接続し、バックエンドプロセスに SQL 文の実行を依頼する。管理者はデータベースアクセス機能の利用に際して、以下の機能を持つ SQL 文を利用することができる。

- データベースの構造定義およびユーザ定義関数の作成
- データのロード
- データのアンロード
- データのバックアップ
- データのリカバリ

管理者および利用者はデータベースアクセス機能の利用に際して、以下の機能を持つ SQL 文を利用することができる。

- データの挿入
- データの更新
- データの削除
- データの参照
- 関数の実行

**■ 監査ログ機能**

管理者や利用者が TOE に行なった操作を記録する。また、管理者は監査ログ機能を用いて監査記録を取得・参照することができる。
管理者は以下の機能を利用することができる。

- 監査ログの取得
- 監査ログの参照

## 2.5. TOE の利用する資源ファイルと保護資産

TOEは、リレーショナルデータベース機能を提供する際に扱うデータを、ＯＳがTOEに割り当てる資源ファイルに格納する。資源ファイルには、データベースデータ、ログファイル、作業用ファイル、動作環境ファイルと言った４種類の形式がある（参照：図 2.2　TOEの論理構成)。データベースデータにはTOEが保護対象とする利用者のデータが格納される。また、データベースデータにはTOEがその機能を提供する際に用いる管理情報も格納される。この論理的な用途を区別して以降では、データベースデータの内、前者を格納するファイルをデータベーススペース、後者を格納するファイルをシステムカタログと呼ぶ。

資源ファイルの内、TOE を介し SQL 文によるアクセスが可能なデータが格納されているのは、データベースデータ（データベーススペースとシステムカタログ）およびログファイルである。作業用ファイル、動作環境ファイルには SQL 文を用いてアクセスすることはできない。

データベースデータの内、TOE を介して利用者がアクセスするのはデータベーススペースのみである。即ち、データベーススペースが本 TOE の保護資産である。一方、データベーススペース以外の資源ファイルは、TOE の機能あるいはセキュリティ機能を実現するために利用する資源である。

### ■ データベーススペース

利用者のデータが表の形式で格納されている資源ファイル。データベーススペースには、論理的なアクセスの単位である表が格納されており、利用者のデータはこの表に格納される。

利用者データへのアクセスを目的とする SQL 文が埋め込まれたアプリケーションが実行されると接続されたバックエンドプロセスが表単位に論理的なアクセスを行う。

本 ST の運用環境では、利用者のデータを格納する表（データベース）は、管理者が SQL 文を用いてデータベーススペース内に作成・定義する。

### ■ システムカタログ

データベースデータに格納されるデータの構造定義情報、利用者の識別認証情報・権限情報、セキュリティパラメタや関数の定義が表の形式で格納されている資源ファイル。これらの表は TOE のインストール時に生成される。データの構造定義情報は、利用者のデータを格納する表（データベース）の論理的な構造を定義したものである。

本 ST の運用環境では、データの構造定義情報は、管理者がデータベースをデータスペース内に作成・定義する際に、システムカタログ内に定義される。このデータの構造定義情報は、利用者ないし管理者がデータベースへアクセスする際に TOE によって参照される。

本 ST の運用環境では、利用者の識別認証情報・権限情報は管理者が SQL 文を用いて登録する。

関数の定義とは利用者がバックエンドプロセスで実行できるよう定義・登録した処理のリストである。関数では、表に対する挿入、更新、削除、参照などの処理を行なうことができる。また、管理者は OS の機能を関数から利用可能なように登録することができる。

本 ST の運用環境では、関数は管理者が SQL 文を用いて定義する。また、OS 機能の利用登録は管

理者がセキュリティ上の安全性を確認した上で SQL 文を用いて登録する。

■ **ログファイル**

データベーススペース、システムカタログの整合性を保証するための更新ログ、およびデータベースデータへのアクセスの際の利用者および管理者の処理記録などの監査ログ、利用者のデータのバックアップが格納されている資源ファイル。アクセスには管理者権限が必要である。

■ **作業用ファイル**

TOEがリレーショナルデータベース機能を提供する際に扱うデータを一時的に格納する資源ファイル。データベーススペース、システムカタログ、ログファイルを操作した時点で、処理途中の整列結果等が一時的に格納されたり、利用者のデータ処理途中に生成される中間データが格納されたりする。作業用ファイルは TOE が内部的に利用する資源ファイルであり、アプリケーション等が TOE の機能を介してアクセスすることはできない。さらに OS の機能においても、アプリケーションのプロセスは TOE および資源ファイルとは分離されているため、アプリケーションが OS の機能を用いてアクセスすることもできない。

管理者は、OS にログインし OS のコマンドを用いて作業ファイルにアクセスすることができる。

■ **動作環境ファイル**

アプリケーションの実行時の動作を定義し、アプリケーションがデータベースデータにアクセスする振る舞いを決定する情報が格納されている資源ファイル。この資源ファイルに TOE を介して（SQL 文）アクセスすることはできない。

動作環境ファイルは、管理者が OS のコマンドを用いてアクセスする。

# 3. TOE セキュリティ環境

本 TOE に対するセキュリティ環境について述べる。

## 3.1. 前提条件

TOE は、以下のような使用環境を想定する。

- **A.MANAGER 管理者の正当性**
  管理者は、不正を行わない。
- **A.USER 利用者による管理**
  利用者は、TOE の利用者識別に際して、利用者自身がアプリケーションを介して使用する識別情報や、利用者がアプリケーションに埋め込んで使用する識別情報を漏洩させない。
- **A.PHYSICAL 物理的な保護**
  管理者以外はTOEの動作するサーバマシンに対し物理的なアクセスはできない。
- **A.OS OS による保護**
  管理者以外はTOEの動作するサーバのOSへログインすることはできない。
  TOE が OS から獲得する資源ファイルの保護は OS が行う。
  管理者は、TOE の保護資産に OS 機能を用いてアクセスする関数の登録をしない。
- **A.TCP TCP/IP ソケットを経由した利用の停止**
  TOE の機能を TCP/IP ソケットを経由して利用する機能を停止する。

## 3.2. 脅威

本 ST では攻撃者の攻撃能力を低レベルと想定する。
TOE に対して以下の脅威を想定する。

- **T.ACCESS アプリケーションを使用したデータベースへの結合**
  TOE への結合を許可されていない者が、TOE の機能を使用して、保護資産への許可されていない操作を行う。あるいは利用者が TOE の機能を使用して、保護資産への許可されていない操作を行う。

## 3.3. 組織のセキュリティ方針

組織のセキュリティポリシーはない。

# 4. セキュリティ対策方針

TOE のセキュリティ対策方針と、環境のセキュリティ対策方針について述べる。

## 4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針について述べる。

- **O.CONNECT 識別と認証**
  TOE は、TOE への結合を許可された利用者および管理者を管理し、利用者および管理者が TOE への結合を要求した場合は、識別および認証を行うことによって、結合を許可されていない者の結合を制限する。
- **O.ACCESS アクセス制御**
  TOE は、TOE への結合を許可された利用者および管理者の、許可された操作および許可された保護資産への操作を管理し、利用者の許可されていない操作、許可されていない保護資産への操作を制限する。

## 4.2. 環境のセキュリティ対策方針

環境のセキュリティ対策方針について述べる。

- **OE.ASSIGN 管理者の選任と管理**
  責任者は、セキュリティシステムの全責任を担う者であり、TOE の管理、および、TOE が想定するセキュアな環境の管理にふさわしい人間を、管理者として選任し、教育や管理を実施しなければならない。
- **OE.USER 管理者による利用者の教育**
  管理者は、利用者に対し、識別情報が漏洩しないよう適切に管理すること、さらに、アプリケーションが他人に利用されたり、アプリケーションの利用を通じて識別情報が漏洩したりすることがないよう指導、教育しなければならない。
- **OE.PHYSICAL 管理者による物理的環境の管理**
  管理者は、TOE の動作するサーバマシンが管理者以外に利用されないようにサーバマシン設置場所への入退室管理、サーバマシンが設置されるラックの施錠管理など適切に実施しなければならない。
- **OE.OS OS を利用した保護環境の管理**
  管理者は管理者以外が OS にログインできないように OS の設定を維持､管理しなければならない。
  管理者は利用者のアプリケーションを TOE の動作する OS 上に設置するに際して､アプリケーションと TOE のリソースを分離し､TOE の資源ファイルやリソースが TOE 以外のプロセス等から直接アクセスされないように OS の機能を用いて設定を維持、管理しなければならない。
  また、アプリケーションのソース等から識別情報が漏洩することがないよう OS の機能やアプリケーションの実行時機能を用いて適切な設定を維持、管理しなければならない。

管理者は OS の手続き言語によって記述された関数を登録する際に、関数が OS の機能を用いて直接 TOE の保護資産にアクセスしないことを検証しなければならない。また、OS の機能を用いて直接保護資産を操作する関数は登録しない。

- **OE.TCP　　TCP/IP ソケットを用いた接続の管理**

  管理者は TCP/IP ソケットが利用するポートを管理する。TOE に対しては TCP/IP ソケットの利用を不可とする。

# 5. ＩＴセキュリティ要件

TOE のセキュリティ要件およびＩＴ環境に対するセキュリティ要件について述べる。

## 5.1. TOE セキュリティ要件

TOE のセキュリティ要件について述べる。

### 5.1.1. TOE セキュリティ機能要件

セキュリティ機能要件について述べる。

セキュリティ機能要件の一覧を「表 5.2　セキュリティ機能要件一覧 (p.44)」に示す。

#### 5.1.1.1. 認証と識別

**1)　　認証失敗(FIA_AFL)**

**管理: FIA_AFL.1**

以下のアクションは FMT における管理機能と考えられる:

a) 不成功の認証試行に対する閾値の管理

b) 認証失敗の事象においてとられるアクションの管理

**監査: FIA_AFL.1**

a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。

**FIA_AFL.1 認証失敗時の取り扱い**

**FIA_AFL.1.1**

TSF は、[割付: *認証事象のリスト*]に関して、[選択: [割付: *正の整数値*], 「[割付: *許容可能な値の範囲*]*内における管理者設定可能な正の正数値*」]回の不成功認証試行が生じたときを検出しなければならない。

[割付] *認証事象のリスト*

アプリケーションからの結合依頼

[選択]　[割付:*正の整数値*]、[割付: *許容可能な値の範囲*]内における管理者設定可能な正の整数値

－　[割付: *正の整数値*]

[割付] *正の整数値*

－　1

**FIA_AFL.1.2**

不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしな

ければならない。
[割付] *アクションのリスト*
－ 結合依頼を拒否し、対象の利用者と事象発生時刻を監査ログとして取得する。
依存性：FIA_UAU.1 認証のタイミング

### 2) 利用者属性定義(FIA_ATD)

**管理: FIA_ATD.1**
以下のアクションは FMT における管理機能と考えられる:
a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。

**監査: FIA_ATD.1**
予見される監査対象事象はない。

**FIA_ATD.1 利用者属性定義**
**FIA_ATD.1.1**
TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:*セキュリティ属性のリスト*]を維持しなければならない。
[割付] *セキュリティ属性のリスト*
－ 資源属性
－ 操作属性
－ 資源量属性
依存性：なし

### 3) 秘密についての仕様(FIA_SOS)

**管理: FIA_SOS.1**
以下のアクションは FMT における管理機能と考えられる:
a) 秘密の検証に使用される尺度の管理。

**監査: FIA_SOS.1**
b) 基本: TSF による、テストされた秘密の拒否または受け入れ;

**FIA_SOS.1 秘密の検証**
**FIA_SOS.1.1**
TSF は、秘密が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければなら

ない。

[割付] *定義された品質尺度*

－ パスワードが従う品質基準は以下のとおり

- パスワードは以下の文字から構成される文字列定数である
  - 英字
  - 数字
  - 以下の特殊文字

    , ( ) . : ; = * + - / ? < > % _ ' "

  - 以下の拡張文字

    @ ¥ #

- パスワードはセキュリティパラメタで指定されるパスワードの最低長（デフォルト:８ 最大値:２５５）以上であり、かつパスワードを構成する文字を４つのクラス（数字、大文字の英字、小文字の英字、それ以外）に分類した際に、それぞれのクラスの文字を含まなければならない。
- あるいは、構成する文字のクラス数が４より小さい場合は、パスワード長はクラス数が少ない分、最低長よりも長くなければならない。
- パスワードを変更する際には、大文字と小文字を同一の文字とみなして新旧を比較した場合、両者が同一、一方が他方を反転したもの、一方が他方を包含するものであってはならない。

依存性：なし

### 4) 利用者認証(FIA_UAU)

**管理: FIA_UAU.2(1)**

以下のアクションは FMT における管理機能と考えられる。

管理者による認証データの管理;

このデータに関係する利用者による認証データの管理。

**監査: FIA_UAU.2(1)**

基本: 認証メカニズムのすべての使用。

**FIA_UAU.2(1) アクション前の利用者認証**

**FIA_UAU.2.1(1)**

TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性：FIA_UID.1 識別のタイミング

### 5) 利用者識別(FIA_UID)

**管理: FIA_UID.2(1)**

以下のアクションは FMT における管理機能と考えられる:

a) 利用者識別情報の管理。

**監査: FIA_UID.2(1)**

b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。

**FIA_UID.2(1) アクション前の利用者識別**

**FIA_UID.2.1(1)**

TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性：なし

### 6) 利用者・サブジェクト結合(FIA_USB)

**管理: FIA_USB.1**

以下のアクションは FMT における管理機能と考えられる:

a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。

b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。

**監査: FIA_USB.1**

b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)。

**FIA_USB.1 利用者・サブジェクト結合**

**FIA_USB.1.1**

TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない：[割付: *利用者セキュリティ属性のリスト*]

[割付] *利用者セキュリティ属性のリスト*

- 資源属性
- 操作属性
- 資源量属性

**FIA_USB.1.2**

TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する

次の規則を実施しなければならない: [割付: *属性の最初の関連付けに関する規則*]

[割付] *属性の最初の関連付けに関する規則*

なし

**FIA_USB.1.3**

TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: *属性の変更に関する規則*]

[割付] *属性の変更に関する規則*

なし

依存性: FIA_ATD.1 利用者属性定義

#### 5.1.1.2. アクセス制御

#### 1) アクセス制御方針(FDP_ACC)

**管理: FDP_ACC.1(1)**

予見される管理アクティビティはない。

**監査: FDP_ACC.1(1)**

予見される監査対象事象はない。

**FDP_ACC.1(1) サブセットアクセス制御**

**FDP_ACC.1.1(1)**

TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]

[割付] *サブジェクト*

－ バックエンドプロセス

[割付] *オブジェクト*

－ 表

－ シーケンス

－ 関数

[割付] *SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*

－ 表に対するデータの参照

－ 表に対するデータの挿入

－ 表に対するデータの更新

－ 表に対するデータの削除
－ シーケンスの参照
－ 関数の実行

[割付] *アクセス制御 SFP*

－ アクセス制御 SFP_DBM

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

**管理: FDP_ACC.1(2)**

予見される管理アクティビティはない。

**監査: FDP_ACC.1(2)**

予見される監査対象事象はない。

**FDP_ACC.1(2) サブセットアクセス制御**

**FDP_ACC.1.1(2)**

TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]

[割付] *サブジェクト*

－ バックエンドプロセス

[割付] *オブジェクト*

－ 表
－ シーケンス
－ 関数

[割付] *SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*

－ 表に対するデータの参照
－ 表に対するデータの挿入
－ 表に対するデータの更新
－ 表に対するデータの削除
－ シーケンスの参照
－ 関数の実行

[割付] *アクセス制御 SFP*

－ アクセス制御 SFP_DBU

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

### 2) アクセス制御機能(FDP_ACF)

**管理: FDP_ACF.1(1)**

以下のアクションは FMT における管理機能と考えられる:

a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。

**監査: FDP_ACF.1(1)**

b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。

**FDP_ACF.1(1) セキュリティ属性によるアクセス制御**

**FDP_ACF.1.1(1)**

TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または、SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または、SFP 関連セキュリティ属性の名前付けされたグループ*]

[割付] *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト*

サブジェクトのリスト

－ バックエンドプロセス

オブジェクトのリスト

－ 表

－ シーケンス

－ 関数

[割付] *各々に対応する、SFP 関連セキュリティ属性、または、SFP 関連セキュリティ属性の名前付けされたグループ*

サブジェクトに対応する SFP 関連セキュリティ属性

－ 利用者属性

－ 資源属性

－ 操作属性

オブジェクトに対応する SFP 関連セキュリティ属性

なし

SFP 関連セキュリティ属性の名前付けされたグループ

－ 管理者権限リスト

[割付] *アクセス制御 SFP*

－ アクセス制御 SFP_DBM

**FDP_ACF.1.2(1)**

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。

[割付] *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*

－ バックエンドプロセスが表を操作する際、および操作にあたってシーケンス、関数を参照する際には、各々に対して操作権限、参照権限が管理者権限リストに登録されていれば許可する

**FDP_ACF.1.3(1)**

TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。

[割付] *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*

なし

**FDP_ACF.1.4(1)**

TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付] *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*

なし

依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

**管理: FDP_ACF.1(2)**

以下のアクションは FMT における管理機能と考えられる:

a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。

**監査: FDP_ACF.1(2)**

b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。

**FDP_ACF.1(2) セキュリティ属性によるアクセス制御**

**FDP_ACF.1.1(2)**

TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び*

*各々に対応する、SFP 関連セキュリティ属性、または、SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または、SFP 関連セキュリティ属性の名前付けされたグループ*]
[割付] *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト*
サブジェクトのリスト
－ バックエンドプロセス
オブジェクトのリスト
－ 表
－ シーケンス
－ 関数
[割付] *各々に対応する、SFP 関連セキュリティ属性、または、SFP 関連セキュリティ属性の名前付けされたグループ*
サブジェクトに対応する SFP 関連セキュリティ属性
－ 利用者属性
－ 資源属性
－ 操作属性
オブジェクトに対応する SFP 関連セキュリティ属性
なし
SFP 関連セキュリティ属性の名前付けされたグループ
－ 権限リスト
[割付] *アクセス制御 SFP*
－ アクセス制御 SFP_DBU

**FDP_ACF.1.2(2)**
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付] *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*
－ バックエンドプロセスが表を操作する際、および操作にあたってシーケンス、関数を参照する際には、各々に対して操作権限、参照権限が権限リストに登録されていれば許可する

**FDP_ACF.1.3(2)**
TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。

[割付] *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*
なし

**FDP_ACF.1.4(2)**
TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付] *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*
なし
依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

#### 5.1.1.3. 資源量の制限

### 1) 資源割当て(FRU_RSA)

**管理: FRU_RSA.1**
以下のアクションは FMT における管理機能と考えられる:
a) グループ及び/または個々の利用者及び/またはサブジェクトに対して、管理者が資源の最大限度を特定すること。

**監査: FRU_RSA.1**
a) 最小: 資源制限による割当て操作の拒否。

**FRU_RSA.1 最大割当て**
**FRU_RSA.1.1**
TSF は、[選択: *個々の利用者、定義された利用者のグループ、サブジェクト*]が[選択: *同時に、特定した時間の間*]使用できる、以下の資源[割付: *制御下にある資源*]の最大割当てを実施しなければならない。
[選択] *個々の利用者、定義された利用者のグループ、サブジェクト*
－ サブジェクト
[選択] *同時に、特定した時間の間*
－ 同時に
[割付] *制御下にある資源*
－ データベーススペース
－ システムカタログ

－ ログファイル
－ 作業用ファイル
－ アプリケーションのプロセスに対応するバックエンドプロセス
依存性：なし

#### 2) 複数同時セションの制限(FTA_MCS)

**管理: FTA_MCS.2**
以下のアクションは FMT における管理機能と考えられる:
a) 管理者による最大許可同時利用者セション数運営規則の管理。

**監査: FTA_MCS.2**
a) 最小: 複数同時セションの制限に基づく新しいセションの拒否。

**FTA_MCS.2 複数同時セションの利用者属性ごと制限**
**FTA_MCS.2.1**
TSF は、規則[割付: *最大同時セション数の規則*]に従って、同一利用者に属する同時セションの最大数を制限しなければならない。
[割付] *最大同時セション数の規則*
－ 管理者が各利用者に対して制限した値

**FTA_MCS.2.2**
TSF は、デフォルトで、利用者あたり[割付: *デフォルト数*]セションの制限を実施しなければならない。
[割付] *デフォルト数*
－ 管理者が、運用に応じて指定する値。省略値＝無制限。範囲＝0～2147483647、または無制限。
依存性: FIA_UID.1 識別のタイミング

#### 5.1.1.4. 資源保護

#### 1) TSF データの管理(FMT_MTD)

**管理: FMT_MTD.1(1)**
以下のアクションは FMT における管理機能と考えられる:
a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。

**監査: FMT_MTD.1(1)**
a) 基本: TSF データの値のすべての改変。

**FMT_MTD.1(1) TSF データの管理**

**FMT_MTD.1.1(1)**

TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]]する能力を[割付:*許可された識別された役割*]に制限しなければならない。

[割付] *TSF データのリスト*

－ システムカタログ

－ ログファイル

[選択] *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]

－ 問い合わせ

[割付] *許可された識別された役割*

－ 管理者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

#### 5.1.1.5. 監査

### 1) セキュリティ監査データ生成(FAU_GEN)

**管理: FAU_GEN.1、FAU_GEN.2**

予見される管理アクティビティはない。

**監査: FAU_GEN.1、FAU_GEN.2**

予見される監査対象事象はない。

**FAU_GEN.1 監査データ生成**

**FAU_GEN.1.1**

TSF は、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択: *最小*、*基本*、*詳細*、*指定なし*: から一つのみ選択]レベルのすべての監査対象事象; 及び

c) [割付: *上記以外の個別に定義した監査対象事象*]。

[選択] *最小*、*基本*、*詳細*、*指定なし*

－ 指定なし

[割付] *上記以外の個別に定義した監査対象事象*

－ 「表 5.4 監査要件」で定義される監査項目

**FAU_GEN.1.2**

TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: *その他の監査関連情報*]

[割付] *その他の監査関連情報*

－ 「表 5.4 監査要件」で定義される監査事象毎の付加情報

依存性: FPT_STM.1 高信頼タイムスタンプ

**FAU_GEN.2 利用者識別情報の関連付け**

**FAU_GEN.2.1**

TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性: FAU_GEN.1 監査データ生成

FIA_UID.1 識別のタイミング

**2) セキュリティ監査レビュー(FAU_SAR)**

**管理: FAU_ SAR.1**

以下のアクションは FMT における管理機能と考えられる:

a) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。

**監査: FAU_ SAR.1**

a) 基本: 監査記録からの情報の読み出し。

**FAU_SAR.1 監査レビュー**

**FAU_SAR.1.1**

TSF は、[割付: *許可利用者*]が、[割付: *監査情報のリスト*]を監査記録から読み出せるようにしなければならない。

[割付] *許可利用者*

－ 管理者

[割付] *監査情報のリスト*

－ 「表 5.4 監査要件」で定義される監査事象毎の監査項目および付加情報

**FAU_SAR.1.2**

TSFは、管理者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

※ 下線部は詳細化

依存性: FAU_GEN.1 監査データ生成

**管理: FAU_SAR.2**

予見される管理アクティビティはない。

**監査: FAU_SAR.2**

a) 基本: 監査記録からの成功しなかった情報読み出し。

**FAU_SAR.2 限定監査レビュー**

**FAU_SAR.2.1**

TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

依存性: FAU_SAR.1 監査レビュー

**管理: FAU_SAR.3**

予見される管理アクティビティはない。

**監査: FAU_SAR.3**

a) 詳細: 閲覧に使用されるパラメタ。

**FAU_SAR.3 選択可能監査レビュー**

**FAU_SAR.3.1**

TSF は、[割付: *論理的な関連の基準*]に基づいて、監査データを[選択: *検索*、*分類*、*並べ替え*]する能力を提供しなければならない。

[割付] *論理的な関連の基準*

－ 監査データの任意の情報（文字列や数値）の大小関係や同値関係

［選択］*検索*、*分類*、*並べ替え*

－ 検索

－ 分類

－ 並べ替え

依存性: FAU_SAR.1 監査レビュー

### 3) セキュリティ監査事象格納(FAU_STG)

**管理: FAU_ STG.1**

予見される管理アクティビティはない。

**監査: FAU_ STG.1**

予見される監査対象事象はない。

**FAU_STG.1 保護された監査証跡格納**

**FAU_STG.1.1**

TSF は、格納された監査記録を不正な削除から保護しなければならない。

**FAU_STG.1.2**

TSF は、監査証跡内の格納された監査記録への不正な改変を[選択: *防止*、*検出*: から一つのみ選択]できねばならない。

[選択: *防止*、*検出*]

－ 防止

依存性: FAU_GEN.1 監査データ生成

**管理: FAU_ STG.4**

以下のアクションは FMT における管理機能と考えられる:

a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。

**監査: FAU_ STG.4**

a) 基本: 監査格納失敗によってとられるアクション。

**FAU_STG.4 監査データ損失の防止**

**FAU_STG.4.1**

TSF は、監査証跡が満杯になった場合、[選択: *監査対象事象の無視*、*特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止*、*最も古くに格納された監査記録への上書き*: から一つのみ選択]及び[割付: *監査格納失敗時にとられるその他のアクション*]を行わねばならない。

[選択] *監査対象事象の無視*、*特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止*、*最も古くに格納された監査記録への上書き*

－ 最も古くに格納された監査記録への上書き

[割付] *監査格納失敗時にとられるその他のアクション*

－ コンソールへのメッセージ出力

依存性: FAU_STG.1 保護された監査証跡格納

#### 5.1.1.6. セキュリティ管理

### 1) TSF における機能の管理(FMT_MOF)

**管理: FMT_MOF.1**

以下のアクションは FMT における管理機能と考えられる:

a) TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること;

**監査: FMT_MOF.1**

a) 基本: TSF の機能のふるまいにおけるすべての改変。

**FMT_MOF.1 セキュリティ機能のふるまいの管理**

**FMT_MOF.1.1**

TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。

[割付] *機能のリスト*

- 認証識別
- アクセス制御
- 資源量の制限
- 資源保護

[選択] *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*

- のふるまいを決定する
- のふるまいを改変する
- を停止する
- を動作させる

[割付] *許可された識別された役割*

- 管理者

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

### 2) セキュリティ属性の管理(FMT_MSA)

**管理: FMT_MSA.1**

以下のアクションは FMT における管理機能と考えられる:

a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。

**監査: FMT_MSA.1**

a) 基本: セキュリティ属性の値の改変すべて。

**FMT_MSA.1 セキュリティ属性の管理**

**FMT_MSA.1.1**

TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、[割付: *その他の操作*]]をする能力を[割付: *許可された識別された役割*]に制限するために[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。

[割付] *セキュリティ属性のリスト*

- 利用者属性
- 資源属性
- 操作属性
- 資源量属性

[選択] *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、[割付: *その他の操作*]

- デフォルト値変更
- 問い合わせ
- 改変
- 削除

[割付] *許可された識別された役割*

- 管理者

[割付] *アクセス制御 SFP*、*情報フロー制御 SFP*

- アクセス制御 SFP_DBU

依存性: [FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

**管理: FMT_MSA.3(1)**

以下のアクションは FMT における管理機能と考えられる:

a) 初期値を特定できる役割のグループを管理すること;

b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。

**監査: FMT_MSA.3(1)**

a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。

b) 基本: セキュリティ属性の初期値の改変すべて。

**FMT_MSA.3(1) 静的属性初期化**

**FMT_MSA.3.1(1)**

TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択: *制限的*、*許可的：から一つのみ選択*、*[割付: その他の特性]*]デフォルト値を与える[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。

[選択] *制限的*、*許可的: から一つのみ選択*、*[割付:その他の特性]*

－ 許可的

[割付] *アクセス制御 SFP*、*情報フロー制御 SFP*

－ アクセス制御 SFP_DBM

**FMT_MSA.3.2(1)**

TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付] *許可された識別された役割*

－ なし

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

**管理: FMT_MSA.3(2)**

以下のアクションは FMT における管理機能と考えられる:

a) 初期値を特定できる役割のグループを管理すること;

b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。

**監査: FMT_MSA.3(2)**

a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。

b) 基本: セキュリティ属性の初期値の改変すべて。

**FMT_MSA.3(2) 静的属性初期化**

**FMT_MSA.3.1(2)**

TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択: *制限的*、*許可的: から一つのみ選択*、*[割付:その他の特性]*]デフォルト値を与える[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。

[選択] *制限的*、*許可的: から一つのみ選択*、*[割付:その他の特性]*

－ 制限的

[割付] *アクセス制御 SFP*、*情報フロー制御 SFP*

－ アクセス制御 SFP_DBU

**FMT_MSA.3.2(2)**

TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付] *許可された識別された役割*

－ なし

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

### 3) TSF データの管理(FMT_MTD)

**管理: FMT_MTD.1(2)**

以下のアクションは FMT における管理機能と考えられる:

a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。

**監査: FMT_MTD.1(2)**

a) 基本: TSF データの値のすべての改変。

**FMT_MTD.1(2) TSF データの管理**

**FMT_MTD.1.1(2)**

TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]]する能力を[割付:*許可された識別された役割*]に制限しなければならない。

[割付] *TSF データのリスト*

－ システムカタログ、動作環境ファイル（「表 5.3 管理要件パラメター覧」で与えられる以下の管理項目）

利用者毎の属性

- 使用可能資源量
- 同時使用セション数

－ ログファイル（「表 5.4 監査要件」で与えられる監査項目）

[選択] *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]

－ デフォルト値変更

－ 削除

[割付] *許可された識別された役割*

－ 管理者

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

**管理: FMT_MTD.1(3)**

以下のアクションは FMT における管理機能と考えられる:

a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。

**監査: FMT_MTD.1(3)**

a) 基本: TSF データの値のすべての改変。

**FMT_MTD.1(3) TSF データの管理**

**FMT_MTD.1.1(3)**

TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]]する能力を[割付:*許可された識別された役割*]に制限しなければならない。

[割付] *TSF データのリスト*

－ システムカタログ、動作環境ファイル（「表 5.3 管理要件パラメター覧」で与えられる以下の管理項目）

利用者毎の属性

- 権限
- 使用可能資源量
- 同時使用セション数

識別認証情報

- 認証情報
- 利用者一覧

[選択] *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]

－ 問い合わせ

－ 改変

[割付] *許可された識別された役割*

－ 管理者

－ 利用者毎の属性および識別認証情報に関連付けられる利用者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

**管理: FMT_MTD.1(4)**

以下のアクションは FMT における管理機能と考えられる:

a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。

**監査: FMT_MTD.1(4)**

a) 基本: TSF データの値のすべての改変。

**FMT_MTD.1(4) TSF データの管理**

**FMT_MTD.1.1(4)**

TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]]する能力を[割付:*許可された識別された役割*]に制限しなければならない。

[割付] *TSF データのリスト*

－ 動作環境ファイル（「表 5.3 管理要件パラメタ一覧」で与えられる以下の管理項目）

危険値（エレメントサイズ）

－ ログファイル（「表 5.4 監査要件」で与えられる監査項目）

[選択] *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]

－ 問い合わせ

－ 改変

[割付] *許可された識別された役割*

－ 管理者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

**管理: FMT_MTD.3**

予見される管理アクティビティはない。

**監査: FMT_MTD.3**

a) 最小: TSF データのすべての拒否された値。

**FMT_MTD.3 セキュアな TSF データ**

**FMT_MTD.3.1**

TSF は、TSF データとしてセキュアな値だけが受け入れられることを保証しなければならない。

依存性: ADV_SPM.1 非形式的 TOE セキュリティ方針モデル

FMT_MTD.1 TSF データの管理

### 4) セキュリティ属性有効期限(FMT_SAE)

**管理: FMT_SAE.1**

以下のアクションは FMT における管理機能と考えられる:

a) 有効期限がサポートされるはずのセキュリティ属性のリストを管理すること;

b) 有効期限の時間が過ぎたときにとられるアクション。

**監査: FMT_SAE.1**

a) 基本: 属性に対する有効期限の時間の特定;

b) 基本: 属性の有効期限切れによってとられるアクション。

**FMT_SAE.1 時限付き許可**

**FMT_SAE.1.1**

TSF は、[割付: *有効期限がサポートされるはずのセキュリティ属性のリスト*]に対する有効期限の時間を特定する能力を、[割付*: 許可された識別された役割*]に制限しなければならない。

[割付]*有効期限がサポートされるはずのセキュリティ属性のリスト*

- 認証情報

[割付] *許可された識別された役割*

- 管理者

**FMT_SAE.1.2**

これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する有効期限の時間後、[割付: *各々のセキュリティ属性に対してとられるアクションのリスト*]を行えなければならない。

[割付]*各々のセキュリティ属性に対してとられるアクションのリスト*

- 認証情報の無効化により、TOE の利用を不可能にする

依存性: FMT_SMR.1 セキュリティ役割
FPT_STM.1 高信頼タイムスタンプ

### 5) 管理機能の特定(FMT_SMF)

**管理: FMT_SMF.1**

予見される管理アクティビティはない。

**監査: FMT_SMF.1**

a) 最小: 管理機能の使用。

**FMT_SMF.1 管理機能の特定**

**FMT_SMF.1.1**

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない : [割付 : *TSF によって提供されるセキュリティ管理機能のリスト*]。

[割付]*TSF によって提供されるセキュリティ管理機能のリスト*

- 「表 5.3 管理要件パラメタ一覧」で与えられる管理項目を管理する機能

依存性 : なし

### 6) セキュリティ管理役割(FMT_SMR)

**管理: FMT_SMR.1(1)**

以下のアクションは FMT における管理機能と考えられる:

a) 役割の一部をなす利用者のグループの管理。

**監査: FMT_SMR.1(1)**

a) 最小: 役割の一部をなす利用者のグループに対する改変;

**FMT_SMR.1(1) セキュリティ役割**

**FMT_SMR.1.1(1)**

TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。

[割付]*許可された識別された役割*

- 管理者
- 利用者毎の属性および識別認証情報に関連付けられる利用者

**FMT_SMR.1.2(1)**

TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

### 7) タイムスタンプ(FPT_STM)

**管理: FPT_STM.1**

以下のアクションは FMT における管理機能と考えられる:

a) 時間の管理。

**監査: FPT_STM.1**

a) 最小: 時間の変更;

**FPT_STM.1 高信頼タイムスタンプ**

**FPT_STM.1.1**

TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性：なし

### 8) リファレンス調停(FPT_RVM)

**管理: FPT_RVM.1**

予見される管理アクティビティはない。

**監査: FPT_RVM.1**

予見される監査対象事象はない。

**FPT_RVM.1　TSP の非バイパス性**

**FPT_RVM.1.1**

TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性：なし

### 9)　ドメイン分離(FPT_SEP)

**管理: FPT_SEP.1**

予見される管理アクティビティはない。

**監査: FPT_SEP.1**

予見される監査対象事象はない。

**FPT_SEP.1　TSF ドメイン分離**

**FPT_SEP.1.1**

TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

**FPT_SEP.1.2**

TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性：なし

### 5.1.2. TOE セキュリティ保証要件

本 ST にて要求する、TOE に対する保証レベルは EAL1 である。

保証コンポーネント構成を「表 5.1 保証要件コンポーネント一覧」に示す。要求する各保証コンポーネントの保証エレメントはCC Ｐａｒｔ３の要求どおりである。なお、ＡＳＥクラスは、保証レベルに関わらず必須となる保証要件として採用する。

**表 5.1 保証要件コンポーネント一覧**

| クラス | コンポーネント名 |
|---|---|
| 構成管理 | ACM_CAP.1 |
| 配付と運用 | ADO_IGS.1 |
| 開発 | ADV_FSP.1 |
| | ADV_RCR.1 |
| ガイダンス文書 | AGD_ADM.1 |
| | AGD_USR.1 |
| テスト | ATE_IND.1 |

### 5.1.3. TOE セキュリティ機能強度

本 TOE は一般のコマーシャルシステムの中で利用されることを想定しているため、最小機能強度レベルは“SOF-基本”である。

機能強度が適用される TOE セキュリティ機能要件は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2(1)、FIA_UID.2(1)であり、その明示された機能強度は“SOF-中位”である。

## 5.2. ＩＴ環境に対するセキュリティ要件

ＩＴ環境に対するセキュリティ要件について述べる。

### 5.2.1. OS に依存する要件

#### 1) セキュリティ管理役割(FMT_SMR)

**管理: FMT_SMR.1(2)**

以下のアクションは FMT における管理機能と考えられる:

a) 役割の一部をなす利用者のグループの管理。

**監査: FMT_SMR.1(2)**

a) 最小: 役割の一部をなす利用者のグループに対する改変;

**FMT_SMR.1(2) セキュリティ役割**

**FMT_SMR.1.1(2)**

OSは、役割[割付: *許可された識別された役割*]を維持しなければならない。

※ 下線部は詳細化

[割付]*許可された識別された役割*

－ 管理者

**FMT_SMR.1.2(2)**

OSは、利用者を役割に関連づけなければならない。

※ 下線部は詳細化

依存性: FIA_UID.1 識別のタイミング

### 2) セキュリティ属性の管理(FMT_MSA)

**管理: FMT_MSA.3(3)**

以下のアクションは FMT における管理機能と考えられる:

a) 初期値を特定できる役割のグループを管理すること;

b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。

**監査: FMT_MSA.3(3)**

a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。

b) 基本: セキュリティ属性の初期値の改変すべて。

**FMT_MSA.3(3) 静的属性初期化**

**FMT_MSA.3.1(3)**

OSは、そのSFPを実施するために使われるセキュリティ属性として、[選択: *制限的、許可的：から一つのみ選択、[割付:その他の特性]*]デフォルト値を与える[割付: *アクセス制御SFP、情報フロー制御SFP*]を実施しなければならない。

※ 下線部は詳細化

[選択] *制限的、許可的: から一つのみ選択、[割付:その他の特性]*

－ 許可的

[割付] *アクセス制御 SFP、情報フロー制御 SFP*

－ アクセス制御 SFP_AT

**FMT_MSA.3.2(3)**

OSは、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

※ 下線部は詳細化

[割付] *許可された識別された役割*

－ なし

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

### 3) 利用者認証(FIA_UAU)

**管理: FIA_UAU.2(2)**

以下のアクションは FMT における管理機能と考えられる。
管理者による認証データの管理;
このデータに関係する利用者による認証データの管理。

**監査: FIA_UAU.2(2)**

基本: 認証メカニズムのすべての使用。

**FIA_UAU.2(2) アクション前の利用者認証**

**FIA_UAU.2.1(2)**

OSは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。
※ 下線部は詳細化
依存性：FIA_UID.1 識別のタイミング

### 4) 利用者識別(FIA_UID)

**管理: FIA_UID.2(2)**

以下のアクションは FMT における管理機能と考えられる:
a) 利用者識別情報の管理。

**監査: FIA_UID.2(2)**

b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。

**FIA_UID.2(2) アクション前の利用者識別**

**FIA_UID.2.1(2)**

OSは、TOEの利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。
※ 下線部は詳細化
依存性：なし

### 5) アクセス制御方針(FDP_ACC)

**管理: FDP_ACC.1(3)**

このコンポーネントについて予見される管理アクティビティはない。

**監査: FDP_ACC.1(3)**

予見される監査対象事象はない。

**FDP_ACC.1(3) サブセットアクセス制御**

**FDP_ACC.1.1(3)**

OSは、[割付: *サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御SFP*]を実施しなければならない。

※ 下線部は詳細化

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]

[割付] *サブジェクト*

－ OS 上で動作する全てのプロセス

[割付] *オブジェクト*

－ データベーススペース

[割付] *SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*

－ データベーススペースに対する読み出し、書き込み

[割付] *アクセス制御 SFP*

－ アクセス制御 SFP_AT

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

### 6) アクセス制御機能(FDP_ACF)

**管理: FDP_ACF.1(3)**

以下のアクションは FMT における管理機能と考えられる:

a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。

**監査: FDP_ACF.1(3)**

b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。

**FDP_ACF.1(3) セキュリティ属性によるアクセス制御**

**FDP_ACF.1.1(3)**

OSは、以下の[割付: *示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び*

*各々に対応する、SFP関連セキュリティ属性、または、SFP関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御SFP*]を実施しなければならない。
※ 下線部は詳細化
[割付] *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト*
サブジェクトのリスト
－ OS 上で動作する全てのプロセス
オブジェクトのリスト
－ データベーススペース
[割付] *各々に対応する、SFP 関連セキュリティ属性、または、SFP 関連セキュリティ属性の名前付けされたグループ*
サブジェクトに対応する SFP 関連セキュリティ属性
－ プロセスの所有者属性
オブジェクトに対応する SFP 関連セキュリティ属性
なし
SFP 関連セキュリティ属性の名前付けされたグループ
－ アクセスパーミッション（OS により、プロセスごとの資源に対する許可操作が定義されたもの）
[割付] *アクセス制御 SFP*
－ アクセス制御 SFP_AT

### FDP_ACF.1.2(3)

OSは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
※ 下線部は詳細化
[割付] *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*
－ OS 上で動作する全てのプロセスの所有者がデータベーススペースを操作する際、アクセスパーミッションで操作を許されているものであれば許可する

### FDP_ACF.1.3(3)

OSは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。
※ 下線部は詳細化
[割付] *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*
なし

**FDP_ACF.1.4(3)**

OSは、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

※ 下線部は詳細化

[割付] *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*

なし

**表 5.2 セキュリティ機能要件一覧**

| セキュリティ機能要件 | |
|---|---|
| 認証、識別 | FIA_AFL.1 |
| | FIA_ATD.1 |
| | FIA_SOS.1 |
| | FIA_UAU.2(1) |
| | FIA_UID.2(1) |
| | FIA_USB.1 |
| アクセス制御 | FDP_ACC.1(1) |
| | FDP_ACF.1(1) |
| | FDP_ACC.1(2) |
| | FDP_ACF.1(2) |
| | FRU_RSA.1 |
| | FTA_MCS.2 |
| | FMT_MTD.1(1) |
| 監査 | FAU_GEN.1 |
| | FAU_GEN.2 |
| | FAU_SAR.1 |
| | FAU_SAR.2 |
| | FAU_SAR.3 |
| | FAU_STG.1 |
| | FAU_STG.4 |
| セキュリティ管理 | FMT_MOF.1 |
| | FMT_MSA.1 |
| | FMT_MSA.3(1) |
| | FMT_MSA.3(2) |
| | FMT_MTD.1(2) |
| | FMT_MTD.1(3) |
| | FMT_MTD.1(4) |
| | FMT_MTD.3 |
| | FMT_SAE.1 |
| | FMT_SMF.1 |
| | FMT_SMR.1(1) |
| | FPT_STM.1 |
| | FPT_RVM.1 |
| | FPT_SEP.1 |
| OS に依存する機能 | FMT_SMR.1(2) |
| | FMT_MSA.3(3) |
| | FIA_UAU.2(2) |
| | FIA_UID.2(2) |
| | FDP_ACC.1(3) |
| | FDP_ACF.1(3) |

**表 5.3 管理要件パラメター覧**

| セキュリティ機能要件 | | 管理要件 | 管理項目 |
|---|---|---|---|
| 認証、識別 | FIA_AFL.1 | 不成功の認証試行に対する閾値の管理 | （固定） |
| | | 認証失敗の事象においてとられるアクションの管理 | （固定） |
| | FIA_ATD.1 | もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる | 利用者毎の属性<br>－権限<br>－使用可能資源量 |
| | FIA_SOS.1 | 秘密の検証に使用される尺度の管理 | （固定） |
| | FIA_UAU.2(1) | 管理者による認証データの管理 | 認証情報 |
| | | このデータに関係する利用者による認証データの管理 | 認証情報 |
| | FIA_UID.2(1) | 利用者識別情報の管理 | 利用者一覧 |
| | FIA_USB.1 | 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる<br><br>許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる | 利用者毎の属性<br>－権限<br>－使用可能資源量<br>－同時使用セション数 |
| アクセス制御 | FDP_ACC.1(1) | 予見される管理アクティビティはない | |
| | FDP_ACF.1(1) | 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理 | （固定） |
| | FDP_ACC.1(2) | 予見される管理アクティビティはない | |
| | FDP_ACF.1(2) | 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理 | 利用者毎の属性<br>－権限 |
| | FRU_RSA.1 | グループ及び/または個々の利用者及び/またはサブジェクトに対して、管理者が資源の最大限度を特定すること | 利用者毎の属性<br>－使用可能資源量 |
| | FTA_MCS.2 | 管理者による最大許可同時利用者セション数の管理 | 利用者毎の属性<br>－同時使用セション数 |
| | FMT_MTD.1(1) | TSF データと相互に影響を及ぼし得る役割のグループを管理すること | （固定） |
| 監査 | FAU_GEN.1 | 予見される管理アクティビティはない | |
| | FAU_GEN.2 | 予見される管理アクティビティはない | |
| | FAU_SAR.1 | 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加) | （固定） |
| | FAU_SAR.2 | 予見される管理アクティビティはない | |
| | FAU_SAR.3 | 予見される管理アクティビティはない | |
| | FAU_STG.1 | 予見される管理アクティビティはない | |
| | FAU_STG.4 | 監査格納失敗時にとられるアクションの維持(削除、改変、追加) | （固定） |

| セキュリティ機能要件 | | 管理要件 | 管理項目 |
|---|---|---|---|
| セキュリティ管理 | FMT_MOF.1 | TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること | （固定） |
| | FMT_MSA.1 | セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること | （固定） |
| | FMT_MSA.3(1) | 初期値を特定できる役割のグループを管理すること | （固定） |
| | | 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること | （固定） |
| | FMT_MSA.3(2) | 初期値を特定できる役割のグループを管理すること | （固定） |
| | | 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること | セキュリティの初期値の強弱 |
| | FMT_MTD.1(2) | TSF データと相互に影響を及ぼし得る役割のグループを管理すること | （固定） |
| | FMT_MTD.1(3) | TSF データと相互に影響を及ぼし得る役割のグループを管理すること | （固定） |
| | FMT_MTD.1(4) | TSF データと相互に影響を及ぼし得る役割のグループを管理すること | （固定） |
| | FMT_MTD.3 | 予見される管理アクティビティはない | |
| | FMT_SAE.1 | 有効期限がサポートされるはずのセキュリティ属性のリストを管理すること | 利用者毎の属性<br>－認証情報の有効期限 |
| | | 有効期限の時間が過ぎたときにとられるアクション | （固定） |
| | FMT_SMF.1 | 予見される管理アクティビティはない | |
| | FMT_SMR.1(1) | 役割の一部をなす利用者のグループの管理 | 利用者毎の属性<br>－権限 |
| | FTP_STM.1 | 時間の管理 | （固定） |
| | FPT_RVM.1 | 予見される管理アクティビティはない | |
| | FPT_SEP.1 | 予見される管理アクティビティはない | |

補足　（固定）とは、TOE の場合は変更できない仕様であるため、管理の要件がないことを意味する。

**表 5.4 監査要件**

| セキュリティ機能要件 | | 監査要件 | 監査項目 | 付加される情報 |
|---|---|---|---|---|
| 認証、識別 | FIA_AFL.1 | 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動) | 1）認証失敗<br>2）認証失敗事象の記録 | なし<br>なし |
| | FIA_ATD.1 | 予見される監査対象事象はない | | |
| | FIA_SOS.1 | 基本: TSF による、テストされた秘密の拒否または受け入れ | 1）不適当な認証情報の拒否 | なし |
| | FIA_UAU.2(1) | 基本: 認証メカニズムのすべての使用 | 1）認証成功<br>2）認証失敗 | なし<br>なし |
| | FIA_UID.2(1) | 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用 | 1）認証成功<br>2）認証失敗 | なし<br>なし |
| | FIA_USB.1 | 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功及び失敗) | 1）認証成功<br>2）認証失敗 | なし<br>なし |
| アクセス制御 | FDP_ACC.1(1) | 予見される監査対象事象はない | | |
| | FDP_ACF.1(1) | 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求 | 1）権限チェック成功<br>2）権限チェック失敗 | 権限、アクセス対象<br>権限、アクセス対象 |
| | FDP_ACC.1(2) | 予見される監査対象事象はない | | |
| | FDP_ACF.1(2) | 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求 | 1）権限チェック成功<br>2）権限チェック失敗 | 権限、アクセス対象<br>権限、アクセス対象 |
| | FRU_RSA.1 | 最小: 資源制限による割当て操作の拒否 | 1）最大資源量を超えるかのチェックに該当 | 資源種別 |
| | FTA_MCS.2 | 最小: 複数同時セションの制限に基づく新しいセションの拒否 | 1）同時使用セション数を超えるかのチェックに該当 | なし |
| | FMT_MTD.1(1) | 基本: TSF データの値のすべての改変 | なし | |

| セキュリティ機能要件 | | 監査要件 | 監査項目 | 付加される情報 |
|---|---|---|---|---|
| 監査 | FAU_GEN.1 | 予見される監査対象事象はない | | |
| | FAU_GEN.2 | 予見される監査対象事象はない | | |
| | FAU_SAR.1 | 基本: 監査記録からの情報の読み出し | 1）監査情報の参照 | 監査情報の参照に用いる SQL 文 |
| | FAU_SAR.2 | 基本: 監査記録からの成功しなかった情報読み出し | 1）監査情報の参照の失敗（権限チェック失敗） | 権限、アクセス対象 |
| | FAU_SAR.3 | 詳細: 閲覧に使用されるパラメタ | 1）監査情報の参照に用いる SQL 文 | 監査情報の参照に用いる SQL 文 |
| | FAU_STG.1 | 予見される監査対象事象はない | | |
| | FAU_STG.4 | 基本: 監査格納失敗によってとられるアクション | 1）監査情報量が満杯に達した時にとられる処理 | なし |
| セキュリティ管理 | FMT_MOF.1 | 基本: TSF の機能のふるまいにおけるすべての改変 | 1）セキュリティ機能の変更操作（DDL 文実行、保守・管理用の SQL 文およびコマンドの実行） | セキュリティ機能の変更操作に用いる DDL 文、SQL 文およびコマンドの引数 |
| | FMT_MSA.1 | 基本: セキュリティ属性の値の改変すべて | 1）セキュリティ属性の変更（DDL 文実行） | セキュリティ属性の変更に用いる DDL 文 |
| | FMT_MSA.3(1) | 基本: セキュリティ属性の初期値の改変すべて | なし | |
| | FMT_MSA.3(2) | 基本: セキュリティ属性の初期値の改変すべて | 1）セキュリティ属性の変更（DDL 文実行） | セキュリティ属性の変更に用いる DDL 文 |
| | FMT_MTD.1(2) | 基本: TSF データの値のすべての改変 | 1）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行） | セキュリティ情報の変更に用いる DDL 文およびコマンドの引数 |
| | FMT_MTD.1(3) | 基本: TSF データの値のすべての改変 | 1）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行）<br>2）認証情報の変更（ALTER ROLE 文実行） | セキュリティ情報の変更に用いる DDL 文およびコマンドの引数<br><br>なし |

| セキュリティ機能要件 | | 監査要件 | 監査項目 | 付加される情報 |
|---|---|---|---|---|
| セキュリティ管理 | FMT_MTD.1(4) | 基本: TSF データの値のすべての改変 | 1）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行） | セキュリティ情報の変更に用いる DDL 文およびコマンドの引数 |
| | FMT_MTD.3 | 最小: TSF データのすべての拒否された値 | 1）セキュリティ情報の変更（DDL 文実行） | セキュリティ情報の変更に用いる DDL 文 |
| | FMT_SAE.1 | 基本: 属性に対する有効期限の時間の特定; | 1）認証情報の有効期限の設定（DDL 文実行） | 認証情報の有効期限の設定に用いる DDL 文 |
| | | 基本: 属性の有効期限切れによってとられるアクション | 1）認証情報が有効期限に達した（認証失敗） | なし |
| | FMT_SMF.1 | 最小: 管理機能の使用 | 1）セキュリティ機能の変更操作（DDL 文実行、保守・管理用のコマンドの実行）<br>2）セキュリティ属性の変更（DDL 文実行）<br>3）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行） | セキュリティ機能の変更操作に用いる DDL 文およびコマンドの引数<br>セキュリティ属性の変更に用いる DDL 文<br>セキュリティ情報の変更に用いる DDL 文およびコマンドの引数 |
| | FMT_SMR.1(1) | 最小: 役割の一部をなす利用者のグループに対する改変 | 1）利用者属性の変更（DDL 文実行） | 利用者属性の変更に用いる DDL 文 |

補足 1

FMT_MTD.1(1)について

本来 TSF データが変更されたことを監査ログに取るべきであるが、TSF データの改変はできないため、FMT_MTD.1(1)では、監査項目は存在しない。

補足 2

FMT_MSA.3(1)について

本来セキュリティ属性の初期値が変更されたことを監査ログに取るべきであるが、全ての表にアクセス可能な属性という初期値は変更できない。そのため、「セキュリティ属性の初期値の改変」は行われず、FMT_MSA.3(1)では、監査項目は存在しない。

補足 3

FMT_MTD.1(3)について

ALTER ROLE 文は、結合済みでなければ実行できない文であり、結合中に何度実行しても有効なのは最後に実行したものだけである。セションに関する情報を取得することにより、ALTER ROLE 文を実行したアプリケーション名、時間が分かるため、利用者は認証情報が変更されたことを知ることができ、追跡・対処が可能である。そのため、FMT_MTD.1(3)では、セションに関する情報を ALTER ROLE 文の情報としている。

# 6. TOE 要約仕様

セキュリティ機能としては、以下のような四つの機能をもっている。

１）運用選択機能（F.SEL）
セキュリティ機能のふるまいを変更する機能である。
２）利用者制御機能（F.USER）
各利用者の権限を制御し、指定された権限の範囲での処理を保証し、またその範囲を超えた処理を制限する機能である。
３）資源制御機能（F.RES）
TOE が使用する資源を制御する機能である。
４）監査ログ機能（F.AUDIT）
利用者や管理者が行った処理に関する情報を保持しておく機能である。

## 6.1. TOE セキュリティ機能

### 6.1.1. 運用選択機能（F.SEL）

セキュリティパラメタを使用して、セキュリティ機能のふるまいを変更する機能である。この機能を使用して、セキュリティの強度を変更することができる。

#### 1) パラメタを変更する機能(F.SEL.PARA)

■ **パラメタの種類**

セキュリティパラメタには、以下のものがある。

- 利用者制御機能に関係するパラメタ

利用者のアプリケーションからの SQL 文のアクセス機能も、使用可能な範囲を指定し、運用として不用な機能を抑止するパラメタがある。

■ **パラメタの変更機能**

セキュリティパラメタの設定には、以下のような DDL 文を用いる。DDL 文実行時には、設定値が実行可能な範囲にあるか否かのチェックを行う。

- ALTER ROLE 文

■ **監査ログ**

セキュリティパラメタの設定は、管理者の行為として記録される。DDL 文全体が記録される。

### 6.1.2. 利用者制御機能（F.USER）

各利用者を識別し、権限を制御し、指定された権限の範囲での処理を保証し、さらに範囲を超えた処理を制限する。

- 利用者を登録する機能
- 管理者および利用者を認証識別する機能
- 利用者の権限を制御する機能
- 利用者の資源量を制御する機能
- 利用者の権限を参照する機能

管理者は、スーパユーザであり、その権限を変更することはできない。管理者は、全ての権限を保持し、資源も無制限に使用できる。即ち、管理者の登録、管理者の権限や資源量を制御する機能はない。

#### 1) 利用者の登録機能（F.USER.DEF）

■ **利用者の登録**

認証情報と識別情報を TOE に対して登録する。（識別情報は、６３バイト以内の先頭が英字で始まる英字または数字、もしくは６３バイト以内の日本語文字列でなければならない）

利用者の登録、および登録した情報の変更や破棄には、以下のような DDL 文を用いる。

- 登録　CREATE ROLE 文
- 変更　ALTER ROLE 文
- 破棄　DROP ROLE 文

■ **監査ログ**

これらの文で指定するパラメタ変更は、管理者の行為として DDL 文全体が記録される。

#### 2) 認証識別機能（F.USER.AUTHEN）

■ **認証識別**

TOE はその利用者が TOE に正当に登録されているか、識別と認証を行う。

■ **認証失敗時の動作**

認証に失敗した場合は、結合依頼を拒否する。

■ **利用者による認証情報の変更**

認証情報は利用者自身による変更も可能であり、以下の SQL 文を用いて行う。

- ALTER ROLE 文

■ **認証情報の適合性**

TOE に登録される認証情報は、OS に登録する認証情報と同程度の品質基準を保持していなければならない。検査の対象は以下の通りである。

- 以下の文字で構成される文字列定数で指定されているか
  - 英字
  - 数字
  - 以下の特殊文字
    , ( ) . : ; = * + - / ? < > % _ ’ ”
  - 以下の拡張文字
    @ ¥ #
- パスワードはセキュリティパラメタで指定されるパスワードの最低長（デフォルト:８ 最大値:２５５）以上であり、かつパスワードを構成する文字を４つのクラス（数字、大文字の英字、小文字の英字、それ以外）に分類した際に、それぞれのクラスの文字を含んでいるか
- あるいは、構成する文字のクラス数が４より小さい場合は、パスワード長はクラス数が少ない分、最低長よりも長いか
- パスワードを変更する際には、大文字と小文字を同一の文字とみなして新旧を比較した場合、両者が同一、一方が他方を反転したもの、一方が他方を包含するものであってはならないか

なお、本 TOE セキュリティ機能の機能強度は、SOF－中位 である。

■ **認証情報の有効期限**

長期間に渡って同一の認証情報を使用するのは、漏洩の危険性がある。このため、管理者は、認証情報の有効期限を定義することができる。管理者が定めた期間が過ぎると、利用者に対して認証情報の変更を促したり、利用者が変更しない場合に認証情報を無効化したりすることで TOE の利用を不可能にする。

■ **監査ログ**

以下の事象について、対象となる利用者と事象発生時刻が監査ログの対象となる。

- 認証の成功
- 認証の失敗
- 認証情報の変更

### 3) 権限の制御機能（F.USER.PRIV）

■ **資源へのアクセス**

各資源（データベースデータ）へのアクセスは、バックエンドプロセスが行う。バックエンドプロセスは UNIX ドメインソケットを介してアプリケーションと結合する。バックエンドプロセスは結合時に提示された識別情報に関連付けられるアクセス権限に従ってアクセスを実行する。

■ **権限**

TOE は管理者や利用者に対して権限の制御を行っている。

権限制御の初期値は、管理者に対してはすべての操作を可能、利用者に対してはすべての操作を不可能に設定されている。

管理者は全ての SQL 文および PostgreSQL 関連コマンドの実行権限を持つ。

管理者は必要に応じて利用者に権限を付与し、利用者は管理者から付与される権限の範囲で、表の操作、シーケンスの参照および関数の実行を行う。

**表 6.1 権限と権限が許可する操作**

| 対象者 | 権限 | 操作 | 資源 |
|---|---|---|---|
| 管理者 | 全て | データの保守<br>TOE の起動・停止<br>（PostgreSQL 関連コマンド） | データベースデータ(データベーススペース、システムカタログ)<br>ログファイル |
| 利用者 | ＳＥＬＥＣＴ権 | 表の参照 | データベーススペース |
| | ＵＰＤＡＴＥ権 | 表の更新 | |
| | ＤＥＬＥＴＥ権 | 表の削除 | |
| | ＩＮＳＥＲＴ権 | 表の挿入 | |
| | ＳＥＬＥＣＴ権 | シーケンスの参照 | |
| | ＥＸＥＣＵＴＥ権 | 関数の実行 | |

■ **権限の制御**

利用者に対する権限の付与、あるいは、剥奪は、管理者のみが実行できる。この権限の付与、および付与した権限の剥奪には、以下のような DDL 文を用いる。

- 付与　ＧＲＡＮＴ文
- 剥奪　ＲＥＶＯＫＥ文

■ **権限のチェック**

アプリケーション実行中に、その利用者に対する権限が変更されることを想定して、データベースのアクセス時に毎回、権限のチェックを実施する。

PostgreSQL 関連コマンドは、管理者のみが実行できる。

■ **監査ログ**

以下の事象が監査ログの対象となる。

- 権限のチェック成功
- 権限のチェック失敗

それぞれの事象において、チェックの対象となった、権限、アクセス対象が記録される。

#### 4) 資源量の制御機能(F.USER.RES)

■ **資源量の制御**

管理者は、各利用者が使用可能な資源量を制限する。利用者は管理者が制限する資源量の範囲で、アプリケーションの実行を行う。制限の対象となる資源は以下の通りであり、セション毎に管理されている。また、一人の利用者が同時に使用可能なセション数も管理している。

- データベーススペース
- システムカタログ
- ログファイル
- 作業用ファイル
- アプリケーションのプロセスに対応するバックエンドプロセス

上記の資源量の制御は、セキュリティパラメタにより行う。

**表 6.2 資源量を制御するセキュリティパラメタ**

| 資源 | セキュリティパラメタ | 補足説明 |
|---|---|---|
| 一人の利用者が同時に使用可能なセション数（バックエンドプロセス数) | CONNECTION LIMIT | これら利用者毎の資源量の指定は CREATE ROLE 文、ALTER ROLE 文で設定する。 |
| データベーススペース | max_files_per_process<br>work_mem | セションあたりのファイル数、メモリの量を制限することで、各利用者が使用する作業用ファイル量を制限できる。<br>これらの利用者毎の資源量の指定は動作環境ファイルで設定する。 |
| システムカタログ | | |
| ログファイル | | |
| 作業用ファイル | | |

■ **監査ログ**

使用可能な資源量を超えた獲得は、監査ログの対象となる。この時、獲得しようとした資源の種別が記録される。

#### 5) 権限情報の参照機能(F.USER.REF)

■ **権限情報の参照**

各利用者の識別に必要な情報、保持している権限や、使用可能な資源量は、システムカタログ内に格納される。これらの情報は、SQL 文を使用して参照できる。

管理者は、全利用者に関する情報を参照することができる。利用者は、自分に関する情報のみ参照することができる。

■ **監査ログ**

以下の事象が監査ログの対象となる。

- 権限のチェック成功

- 権限のチェック失敗

それぞれの事象において、チェックの対象となった、権限、アクセス対象が記録される。

### 6.1.3. 資源制御機能（F.RES）

資源制御機能とは、TOE が使用する資源を制御する機能である。

#### 1) 属性の制御機能(F.RES.ATTR)

TSF データの参照は、管理者のみに許可する。

TSF データとは以下のものである。

- システムカタログ
- ログファイル

### 6.1.4. 監査ログ機能（F.AUDIT）

監査ログ機能とは、利用者や管理者の処理の情報を保持しておく機能である。以下の機能からなる。

- 監査ログの取得機能
- 監査ログの参照機能
- 監査ログの領域管理機能

#### 1) 監査ログの取得機能(F.AUDIT.COL)

監査ログの取得の対象となる事象は以下の通りである。

- 利用者による TOE に対する結合と結合解除
- 利用者からの要求によるデータベースへのアクセス
- 管理者による TOE に対する操作
- システムで発生した異常に関する情報

■ **利用者による TOE に対する結合処理と結合解除処理**

利用者による TOE に対する結合処理と結合解除処理の情報を取得する。ただし、管理者がアプリケーションを実行した場合も、情報が取得される。

これらの事象に対して、以下のような情報が取得される。

- 事象の発生した日時
- 認証成功／失敗
- 認証に失敗した場合、失敗した理由
- アプリケーションを識別する情報
- 利用者名
- 結合から結合解除までに行われた処理の要約

■ **利用者からの要求によるデータベースへのアクセス**

利用者からの要求によるデータベースへのアクセス時、権限のチェックの情報を取得する。また、管理者がアプリケーションを実行した場合も、情報が取得される。さらに、SQL 文でアクセス可能なシステムカタログや監査ログの参照に関しても、情報が取得される。

これらの事象に対して、以下のような情報が取得される。

- 事象の発生した日時
- 権限チェック成功／失敗
- アプリケーションを識別する情報
- 利用者名
- アクセス対象の資源

■ **管理者による TOE に対する操作**

管理者による TOE に対する操作の情報を取得する。これは、管理者にのみ許可された機能が誤用された場合の影響が大きいためである。以下の事象がある。

- 保守・管理用の SQL 文または PostgreSQL 関連コマンドの実行
- DDL 文の実行
- 監査ログに対する参照

保守・管理用のコマンドは、システムの起動・停止に使用する。これらの事象に対して、以下のような情報がある。

- 事象の発生した日時
- 管理者の処理を識別する情報（コマンドの引数、SQL 文など）

■ **システムで発生した異常に関する情報**

システムで発生した異常に関する情報には、以下のものがある。

- 監査ログが満杯になった
- 監査ログ量が危険値に達した
- 同時使用セション数を超えた
- 利用者が使用可能な最大資源量を超えた

これらの事象に対して、以下のような情報が取得される。

- アプリケーションを識別する情報
- 利用者名
- 異常事象を識別する情報（エラーメッセージ）

ただし、アプリケーションや利用者と直接関わらない場所で発生した異常事象に関しては、異常事象の主体はシステムと識別され、それらに関する情報は取得されない。

### 2) 監査ログの参照機能（F.AUDIT.VIEW）

管理者は監査ログを読み出して監査記録を表の形式に変換し格納することができる。表の形式で格納された監査記録は SQL 文を使用して参照可能である。SQL 文を用いることによって、条件づけによる情報の絞込みや、取り出し順番を自由に指定することができる。
監査ログを読み出して表の形式に変換する操作は管理者のみ実行可能である。また、表の形式で格納された監査記録に対しては、管理者のみデータベース操作（SQL 文による操作）を可能にする。

### 3) 監査ログ領域管理機能（F.AUDIT.SPACE）

■ **監査ログの領域管理**

監査ログは監査記録を複数個の単位に分割して格納する。この分割の単位をエレメントと呼ぶ。監査ログに対する操作は、エレメント単位に行う。監査ログの作成、追加、参照、削除、バックアップや復元は、エレメント単位に行うことができる。なお、監査ログの作成、追加、参照、削除、バックアップや復元は管理者のみ実行可能である。

TOE は、一つのエレメントに監査ログを取得し、そのエレメントが満杯になると、管理者にその事象を通知した後に、次のエレメントに情報を取得する。管理者は、全てのエレメントが満杯になるまでの間に、いずれかの（通常は最も古い）エレメントをバックアップ、削除する。

■ **監査ログが満杯時の事象**

監査ログの満杯、つまり全てのエレメントが満杯になることは、通常の運用の中では発生しない事象である。これが発生した場合、TOE は最も古くに格納されたエレメントを上書きして TOE の動作および監査ログの取得を継続する。

### 6.1.5. セキュリティ機能要件対応

6.1.1 から 6.1.4 までの TOE セキュリティ機能は、セキュリティ機能要件と下表の通り対応する。

**表 6.3 セキュリティ機能とセキュリティ機能要件**

| セキュリティ仕様概要 / セキュリティ機能要件 | | F.SEL.PARA | F.USER.DEF | F.USER.AUTHEN | F.USER.PRIV | F.USER.RES | F.USER.REF | F.RES.ATTR | F.AUDIT.COL | F.AUDIT.VIEW | F.AUDIT.SPACE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 認証・識別 | FIA_AFL.1 | | | ✓ | | | | | | | |
| | FIA_ATD.1 | | ✓ | | ✓ | ✓ | | | | | |
| | FIA_SOS.1 | | | ✓ | | | | | | | |
| | FIA_UAU.2(1) | | | ✓ | | | | | | | |
| | FIA_UID.2(1) | | | ✓ | | | | | | | |
| | FIA_USB.1 | | | | ✓ | ✓ | | | | | |
| アクセス制御 | FDP_ACC.1(1) | | | | ✓ | | | | | | |
| | FDP_ACF.1(1) | | | | ✓ | | | | | | |
| | FDP_ACC.1(2) | | | | ✓ | | | | | | |
| | FDP_ACF.1(2) | | | | ✓ | | | | | | |
| | FRU_RSA.1 | | | | | ✓ | | | | | |
| | FTA_MCS.2 | | | | | ✓ | | | | | |
| | FMT_MTD.1(1) | | | | | | | ✓ | | | |
| 監査 | FAU_GEN.1 | | | | | | | | ✓ | | |
| | FAU_GEN.2 | | | | | | | | ✓ | | |
| | FAU_SAR.1 | | | | | | | | | ✓ | |
| | FAU_SAR.2 | | | | | | | | | ✓ | |
| | FAU_SAR.3 | | | | | | | | | ✓ | |
| | FAU_STG.1 | | | | | | | | | | ✓ |
| | FAU_STG.4 | | | | | | | | | | ✓ |
| セキュリティ管理 | FMT_MOF.1 | ✓ | | | ✓ | | | | | | |
| | FMT_MSA.1 | | | ✓ | ✓ | ✓ | | | | | |
| | FMT_MSA.3(1) | | | | ✓ | | | | | | |
| | FMT_MSA.3(2) | | | | ✓ | | | | | | |
| | FMT_MTD.1(2) | ✓ | | | ✓ | | | | | | ✓ |
| | FMT_MTD.1(3) | | ✓ | ✓ | ✓ | | ✓ | | | | |
| | FMT_MTD.1(4) | ✓ | | | ✓ | | | | | ✓ | ✓ |
| | FMT_MTD.3 | ✓ | ✓ | ✓ | ✓ | | | | | | |
| | FMT_SAE.1 | | | ✓ | | | | | | | |
| | FMT_SMF.1 | ✓ | | | ✓ | ✓ | | | | ✓ | ✓ |
| | FMT_SMR.1(1) | | ✓ | | | | | | | | |
| | FPT_STM.1 | | | ✓ | | | | | ✓ | ✓ | |

## 6.2. 保証手段

本 ST における保証要件コンポーネント名と保証手段を下表に示す。

**表 6.4 保証要件コンポーネント名と保証手段**

| クラス | コンポーネント名 | 保証手段 |
|---|---|---|
| 構成管理 | ACM_CAP.1 | n/a |
| 配付と運用 | ADO_IGS.1 | －PosgreSQL 認証版セキュリティガイド<br>（含インストール、運用手順） |
| 開発 | ADV_FSP.1<br>ADV_RCR.1 | －セキュリティ機能仕様書<br>（含セキュリティ対応表、セキュリティ用語集） |
| ガイダンス文書 | AGD_ADM.1<br>AGD_USR.1 | －PosgreSQL 認証版セキュリティガイド<br>（含インストール、運用手順） |
| テスト | ATE_IND.1 | －PosgreSQL 認証版セキュリティガイド<br>（含インストール、運用手順）<br>－PostgreSQL Regression Test |

# 7. PP 主張

本 ST に準拠する PP はない。

# 8. 根拠

本 ST で規定した内容についての正当性の主張とその検証について記述する。

## 8.1. セキュリティ対策方針根拠

### 1) 必要性

「表 8.1 前提条件および脅威に対するセキュリティ対策方針」に本STの運用環境における前提条件およびTOEに対する脅威に対しひとつ以上のセキュリティ対策方針で対応していることを示す。

**表 8.1 前提条件および脅威に対するセキュリティ対策方針**

| セキュリティ対策方針 / 前提条件・脅威 | O.CONNECT | O.ACCESS | OE.ASSIGN | OE.USER | OE.PHYSICAL | OE.OS | OE.TCP |
|---|---|---|---|---|---|---|---|
| A.MANAGER | | | ✓ | | | | |
| A.USER | | | | ✓ | | | |
| A.PHYSICAL | | | | | ✓ | | |
| A.OS | | | | | | ✓ | |
| A.TCP | | | | | | | ✓ |
| T.ACCESS | ✓ | ✓ | | | | | |

### 2) 十分性

本 ST の運用環境における前提条件および TOE に対する脅威、各々に対してセキュリティ対策方針を説明する。

- **A.MANAGER の実現**

  前提条件 A.MANAGER は、OE.ASSIGN に示したように、ふさわしい管理者の選任と、その管理者に対する教育により実現する。

- **A.USER の実現**

  前提条件 A.USER は、OE.USER に示したように、管理者が利用者に対し利用者が使用する識別情報が漏洩しないように管理することを指導、教育すること。さらに、アプリケーションが不正に他人に利用される、またアプリケーションの利用を通じて識別情報が漏洩することがないよう指導、教育することで実現する。

  指導や教育の内容には、アプリケーションの不正な利用を防ぐために OS の機能を適切に用いる方法や手段の紹介、識別情報の漏洩を引き起こす事例の紹介とその対策手法・検証手法の教育などが含まれる。

■ **A.PHYSICAL の実現**

前提条件 A.PHYSICAL は、OE.PHYSICAL に示したように、物理的環境の管理により実現する。物理的な環境の管理とは、サーバマシンの設置場所への入退室管理、サーバマシンが設置されるラックの施錠管理などの処置である。

■ **A.OS の実現**

前提条件 A.OS の実現は、OE.OS に示したように、TOE の動作するサーバの OS に管理者以外をログインさせないよう、また、TOE の資源ファイル、プロセス、UNIX ドメインソケット等 TOE が OS から確保する資源を、TOE 以外のプロセスから分離するよう、管理者が OS の設定を維持・管理することにより実現する。

■ **A.TCP の実現**

前提条件 A.TCP の実現は、OE.TCP によって TCP/IP ソケットを用いた TOE への結合を不可能とすることによって実現する。

■ **T.ACCESS に対する対策方針**

結合時に O.CONNECT によって、認証を行い識別情報の正当性を確認することで、TOE への結合を許可されていない者の結合を拒否している。

TOE への結合を許可された利用者が TOE の機能を利用して保護資産にアクセスする方法は、アプリケーションに埋め込まれた SQL 文によるアクセスのみである。

アプリケーションでの SQL 文によるアクセスは、データベース形式のファイル（データベーススペース、システムカタログ）しかアクセスできないため、ログファイル、作業用ファイル、動作環境ファイルの３つのファイルはアクセス不可能である。データベーススペース、システムカタログについては、O.ACCESS によって、TOE は権限の有無をチェックし、権限のないものには処理を禁止している。

また、TOE の運用環境および TOE の動作の異常、あるいは想定外の利用事象は監査ログに記録されるので管理者が検出することができる。

## 8.2. セキュリティ要件根拠

### 1) 必要性

「表 8.2　セキュリティ対策方針に対応するセキュリティ機能要件の一覧」にセキュリティ機能要件が１つ以上のセキュリティ対策方針を満たしていることを示す。

**表 8.2 セキュリティ対策方針に対応するセキュリティ機能要件の一覧**

| セキュリティ機能要件 \ セキュリティ対策方針 | | O.CONNECT | O.ACCESS | OE.OS |
|---|---|---|---|---|
| 認証、識別 | FIA_AFL.1 | ✓ | | |
| | FIA_ATD.1 | ✓ | ✓ | |
| | FIA_SOS.1 | ✓ | | |
| | FIA_UAU.2(1) | ✓ | | |
| | FIA_UID.2(1) | ✓ | | |
| | FIA_USB.1 | ✓ | ✓ | |
| アクセス制御 | FDP_ACC.1(1) | | ✓ | |
| | FDP_ACF.1(1) | | ✓ | |
| | FDP_ACC.1(2) | | ✓ | |
| | FDP_ACF.1(2) | | ✓ | |
| | FRU_RSA.1 | ✓ | | |
| | FTA_MCS.2 | ✓ | | |
| | FMT_MTD.1(1) | | ✓ | |
| 監査 | FAU_GEN.1 | ✓ | ✓ | |
| | FAU_GEN.2 | ✓ | ✓ | |
| | FAU_SAR.1 | | ✓ | |
| | FAU_SAR.2 | | ✓ | |
| | FAU_SAR.3 | | ✓ | |
| | FAU_STG.1 | | ✓ | |
| | FAU_STG.4 | ✓ | ✓ | |
| セキュリティ管理 | FMT_MOF.1 | ✓ | ✓ | |
| | FMT_MSA.1 | | ✓ | |
| | FMT_MSA.3(1) | | ✓ | |
| | FMT_MSA.3(2) | | ✓ | |
| | FMT_MTD.1(2) | | ✓ | |
| | FMT_MTD.1(3) | ✓ | ✓ | |
| | FMT_MTD.1(4) | | ✓ | |
| | FMT_MTD.3 | ✓ | ✓ | |
| | FMT_SAE.1 | ✓ | | |
| | FMT_SMF.1 | ✓ | ✓ | |
| | FMT_SMR.1(1) | ✓ | ✓ | |
| | FPT_STM.1 | ✓ | ✓ | |
| | FPT_RVM.1 | ✓ | ✓ | |
| | FPT_SEP.1 | ✓ | ✓ | |
| OS に依存する機能 | FMT_SMR.1(2) | | | ✓ |
| | FMT_MSA.3(3) | | | ✓ |
| | FIA_UAU.2(2) | | | ✓ |
| | FIA_UID.2(2) | | | ✓ |
| | FDP_ACC.1(3) | | | ✓ |
| | FDP_ACF.1(3) | | | ✓ |

### 2) 十分性

セキュリティ対策方針の各々に対してそれを実現するセキュリティ機能要件を説明する。

■ **全ての対策方針の前提となる機能要件**

FPT_RVM.1 セキュリティ機能要件を採用することにより、TOE の各機能が利用されようとする際には、必ずセキュリティ機能が呼び出されるため、セキュリティ機能を迂回することはできない。
また、FPT_SEP.1 セキュリティ機能要件を採用することにより、TOE の動作空間において利用者がアクセス可能なアプリケーションのプロセスと TOE の各機能が動作するプロセス（コマンド、サーバプロセスおよびバックエンドプロセス）が分離され、セキュリティ機能への不当な干渉を防ぐことができる。
以上により、セキュリティ機能が迂回されたり干渉されたりせず、正しく動作する。

また、認証履歴、セキュリティ機能の操作履歴などの監査記録の取得、認証情報の有効期限管理のためには、正確な時間情報が必要であるが、FPT_STM.1 セキュリティ機能要件を採用することにより、本 TOE は正確な時間情報を一貫して維持利用する。

■ **IT対策方針に対して採用する機能要件**

● **O.CONNECT に対して採用する機能要件**

本 TOE が安全にデータベースサービスを提供するためには、利用者に対して TOE を使用させる前に利用者を識別し、本人であることを認証しなければならない。識別および認証では、TOE が FIA_UID.2(1)セキュリティ機能要件に基づいてその利用者を識別し、その後、FIA_UAU.2(1)セキュリティ機能要件に基づき認証を行う。
FMT_MTD.1(3)セキュリティ機能要件により、管理者は全利用者の認証情報を、利用者は自分自身の認証情報を変更可能である。また、FIA_SOS.1 セキュリティ機能要件を採用することにより、認証情報は TOE が予め定める非類似性品質基準を満たすと共に、管理者がセキュリティパラメタによって指定する複雑さを持つ。さらに、FMT_SAE.1 セキュリティ機能要件を採用することで、管理者は認証情報の有効期限を設定し、定期的な認証情報の更新を強要できる。これらにより、本人以外の利用者が認証情報を推測して利用することは困難となる。
利用者が認証に失敗した際には、FIA_AFL.1 セキュリティ機能要件に基づいて、その事象を監査ログとして取得する。
本TOEは、FMT_SMF.1 セキュリティ機能要件を採用することにより、セキュリティ機能、セキュリティ属性およびTSFデータを管理する機能を持つ。FMT_MOF.1 セキュリティ機能要件を採用することにより、管理者のみセキュリティ機能の振る舞いを決定／改変することができる。ここでは、認証情報の有効期限などを決定／改変することができる。変更するTSFデータの正当性は、FMT_MTD.3 セキュリティ機能要件を採用することでチェックされる。
本 TOE では、識別および認証が完了し、利用者の資源量制御を行う際には、FIA_ATD.1 セキュリティ機能要件を採用することによって、あらかじめ定義された利用者の利用可能な資源量は管理さ

れ、FIA_USB.1 セキュリティ機能要件により利用者と関連付けられる。資源量制御は、この関連付けられた資源量に従って行われる。FTA_MCS.2 セキュリティ機能要件を採用することにより、TOE の機能を利用しようとする全ての利用者に対して、同時に開設することが可能なセション数を制限する。さらに、FRU_RSA.1 セキュリティ機能要件を採用することで、セション毎に使用することができる最大の OS 資源量を制限する。
本 TOE では、管理者、利用者という役割は、FMT_SMR.1(1)により維持される。
本 TOE では、FAU_GEN.1 セキュリティ機能要件を採用することにより、TOE への結合依頼とその認証結果に関する記録を採取する。その記録には、FAU_GEN.2 セキュリティ機能要件に基づき、どの利用者、または管理者の操作の結果として監査対象事象が発生したのかも併せて記録される。
なお、FAU_STG.4 セキュリティ機能要件に基づき、監査記録を記録する監査ログが満杯になった場合には古い監査ログエレメントの上書きを行うため、監査記録が採られなくなることはない。

以上により、利用者の確実な識別および認証が可能である。

- **O.ACCESS に対して採用する機能要件**

本 TOE が安全にデータベースサービスを提供するためには、データベースとデータベースへの操作を制御し、TOE への結合を許可した各利用者に対して、利用者毎の職務権限に応じた割当業務のみを遂行できるように制御するといったように必要最低限のアクセス権限のみを付与しなければならない。
本 TOE では、まず、利用者のアクセス制御を行う際に、FIA_ATD.1 セキュリティ機能要件を採用することによって、あらかじめ定義された利用者の利用可能な資源、操作方法が管理され、FIA_USB.1 セキュリティ機能要件により利用者と関連付けられる。アクセス制御は、この関連付けられた資源、操作方法に従って行われる。
FMT_MSA.3(1)セキュリティ機能要件を採用することにより、表のアクセス権限は、管理者に全て与えられており、FDP_ACC.1(1)および FDP_ACF.1(1)セキュリティ機能要件を採用することにより、利用者は管理者のデータベースへのアクセスが制御される。また、FDP_ACC.1(2)および FDP_ACF.1(2)セキュリティ機能要件を採用することにより、利用者は管理者から付与された権限の範囲でのみデータベースへのアクセスを行う。また、FMT_MSA.3(2)セキュリティ機能要件を採用することにより、管理者のみ表のアクセス権限の初期値を指定でき、FMT_MSA.1 セキュリティ機能要件により、管理者のみ表のアクセス権限を変更できる。
次に、本 TOE は、FMT_SMF.1 セキュリティ機能要件を採用することにより、セキュリティ機能、セキュリティ属性および TSF データを管理する機能を持つ。FMT_MOF.1 セキュリティ機能要件を採用することにより、管理者のみセキュリティ機能の振る舞いを決定／改変することができる。変更する TSF データの正当性は、FMT_MTD.3 セキュリティ機能要件を採用することでチェックされる。

本 TOE が十分な信頼性を確保するためには、アクセス制御が行われるのに必要なアクセス権限を適

切に設定し、正当なアクセス権限をもたない者が資源を盗み見る／改ざんすることを防止することが必要不可欠である。

FMT_MTD.1(1)セキュリティ機能要件により、システムカタログ、ログファイル、作業用ファイルは管理者のみ読み出し可能である。また、FMT_MTD.1(2)セキュリティ機能要件を採用することによって、管理者のみ権限情報、資源量や認証情報の管理を行うことができる。FMT_MTD.3 セキュリティ機能要件を採用することで、変更するこれらの値の正当性がチェックされる。

また、利用者に付与された権限情報や、使用可能な資源量、および識別認証情報は、FMT_MTD.1(3)セキュリティ機能要件により管理者は全利用者の情報を、利用者は自分に関する情報を参照することができる。

本 TOE では、管理者、利用者という役割は、FMT_SMR.1(1)により維持される。

本 TOE では、FAU_GEN.1 セキュリティ機能要件を採用することにより、データベースへの操作、および管理行為に関する記録を採取する。その記録には、FAU_GEN.2 セキュリティ機能要件に基づき、どの利用者、または管理者の操作の結果として監査対象事象が発生したのかも併せて記録される。

監査記録については、FAU_STG.1 セキュリティ機能要件を採用することにより、管理者のみ監査記録の削除を行うことができる。なお、FAU_STG.4 セキュリティ機能要件に基づき、監査記録を記録する監査ログが満杯になった場合には古い監査ログエレメントの上書きを行うため、監査記録が採られなくなることはない。

また、FAU_SAR.1 セキュリティ機能要件を採用することにより、管理者は監査ログを参照して監査記録を分析することができる。また、FAU_SAR.2 セキュリティ機能要件を採用することにより、管理者以外の監査記録へのアクセスを禁止する。なお、監査記録の参照については、FAU_SAR.3 セキュリティ機能要件を採用により、監査分析行為を高精度かつ効率的に遂行するために、管理者は監査記録データに対する整列や検索などを行なうことができる。

また、FMT_MTD.1(4)セキュリティ機能要件を採用することによって、管理者のみ取得する監査情報を選択できる。FMT_MTD.3 セキュリティ機能要件を採用することで、変更するこれらの値の正当性がチェックされる。

以上により、データベースデータおよび監査ログへのアクセス制御が可能である。

■ **非IT対策方針に対して採用する機能要件**

● **OE.OS に対して採用する機能要件**

本 TOE が安定したデータベースサービスを提供維持するためには、TOE が動作する環境が適切であることが必要不可欠である（たとえば TCP/IP ソケット連携を拒否するパラメタを設定する）。

本 ST では OS にログインできるのは管理者のみである。OS は FIA_UID.2(2)セキュリティ機能要件に基づいてその利用者を識別し、その後、FIA_UAU.2(2)セキュリティ機能要件に基づき認証を行う。

本 TOE では、FMT_MSA.3(3) セキュリティ機能要件により、資源ファイルに対しては管理者のみ

アクセス可能であり、FDP_ACC.1(3)および FDP_ACF.1(3)セキュリティ機能要件により、資源ファイルに対して OS によるアクセス制御が行われる。なお、OS の管理者という役割は、FMT_SMR.1(2)により維持される。

以上により、TOE が動作する適切な環境は維持される。

- **OE.TCP に対して採用する機能要件**

  OE.TCP は OS の機能を用いた設定であり、対応するセキュリティ機能要件はない。

### 8.2.1. 依存関係

セキュリティ要件に対する依存関係一覧を下表に示す。

**表 8.3 セキュリティ要件の依存関係一覧**

| 項番 | セキュリティ機能要件 | | 依存する要件 | 参照項番 |
|---|---|---|---|---|
| 1 | 認証、識別 | FIA_AFL.1 | FIA_UAU.2(1) ※1 | 4 |
| 2 | | FIA_ATD.1 | なし | |
| 3 | | FIA_SOS.1 | なし | |
| 4 | | FIA_UAU.2(1) | FIA_UID.2(1) ※1 | 5 |
| 5 | | FIA_UID.2(1) | なし | |
| 6 | | FIA_USB.1 | FIA_ATD.1 | 2 |
| 7 | アクセス制御 | FDP_ACC.1(1) | FDP_ACF.1(1) | 8 |
| 8 | | FDP_ACF.1(1) | FDP_ACC.1(1)<br>FMT_MSA.3(1) | 9<br>23 |
| 9 | | FDP_ACC.1(2) | FDP_ACF.1(2) | 10 |
| 10 | | FDP_ACF.1(2) | FDP_ACC.1(2)<br>FMT_MSA.3(2) | 9<br>24 |
| 11 | | FRU_RSA.1 | なし | |
| 12 | | FTA_MCS.2 | FIA_UID.2(1) ※1 | 5 |
| 13 | | FMT_MTD.1(1) | FMT_SMR.1(1)<br>FMT_SMF.1 | 31<br>30 |
| 14 | 監査 | FAU_GEN.1 | FPT_STM.1 | 32 |
| 15 | | FAU_GEN.2 | FAU_GEN.1<br>FIA_UID.2(1) ※1 | 14<br>5 |
| 16 | | FAU_SAR.1 | FAU_GEN.1 | 14 |
| 17 | | FAU_SAR.2 | FAU_SAR.1 | 16 |
| 18 | | FAU_SAR.3 | FAU_SAR.1 | 16 |
| 19 | | FAU_STG.1 | FAU_GEN.1 | 14 |
| 20 | | FAU_STG.4 | FAU_STG.1 | 19 |
| 21 | セキュリティ管理 | FMT_MOF.1 | FMT_SMR.1(1)<br>FMT_SMF.1 | 31<br>30 |
| 22 | | FMT_MSA.1 | FMT_SMR.1(1)<br>FDP_ACC.1(2)<br>FMT_SMF.1 | 31<br>9<br>30 |
| 23 | | FMT_MSA.3(1) ※2 | FMT_SMR.1(1) | 31 |
| 24 | | FMT_MSA.3(2) | FMT_MSA.1<br>FMT_SMR.1(1) | 22<br>31 |
| 25 | | FMT_MTD.1(2) | FMT_SMR.1(1)<br>FMT_SMF.1 | 31<br>30 |
| 26 | | FMT_MTD.1(3) | FMT_SMR.1(1)<br>FMT_SMF.1 | 31<br>30 |
| 27 | | FMT_MTD.1(4) | FMT_SMR.1(1)<br>FMT_SMF.1 | 31<br>30 |
| 28 | | FMT_MTD.3 | FMT_MTD.1(2)<br>FMT_MTD.1(3)<br>FMT_MTD.1(4)<br>ADV_SPM.1 | 25<br>26<br>27<br>― |
| 29 | | FMT_SAE.1 | FMT_SMR.1(1)<br>FPT_STM.1 | 31<br>32 |

| 項番 | セキュリティ機能要件 | | 依存する要件 | 参照項番 |
|---|---|---|---|---|
| 30 | セキュリティ管理 | FMT_SMF.1 | なし | |
| 31 | | FMT_SMR.1(1) | FIA_UID.2(1) ※1 | 5 |
| 32 | | FPT_STM.1 | なし | |
| 33 | | FPT_RVM.1 | なし | |
| 34 | | FPT_SEP.1 | なし | |
| 35 | OS に依存する機能 | FMT_SMR.1(2) | FIA_UID.2(2) ※1 | 38 |
| 36 | | FMT_MSA.3(3) ※2 | FMT_SMR.1(2) | 35 |
| 37 | | FIA_UAU.2(2) | FIA_UID.2(2) ※1 | 38 |
| 38 | | FIA_UID.2(2) | なし | |
| 39 | | FDP_ACC.1(3) | FDP_ACF.1(3) | 40 |
| 40 | | FDP_ACF.1(3) | FDP_ACC.1(3)<br>FMT_MSA.3(3) | 39<br>36 |

上記の依存関係を確認した。

※1　本来依存する要件は FIA_UID.1 および FIA_UAU.1 だが、本 TOE のセキュリティ機能は FIA_UID.2 および FIA_UAU.2 を必要とするため、ここでは FIA_UID.2 および FIA_UAU.2 としている。

※2　FMT_MSA.3(1)および FMT_MSA.3(3)のセキュリティ属性は固定であり、変更は行われないものであるため、FMT_MSA.1 への依存関係を構築しないものとする。

### 8.2.2. 相互支援

セキュリティ機能要件に対する相互支援一覧を下表に示す。

**表 8.4 セキュリティ要件の相互支援関係一覧**

| セキュリティ機能要件 | | 防御を提供している要件 | | |
|---|---|---|---|---|
| | | 迂回抑止 | 干渉抑止 | 非活性化抑止 |
| 認証、識別 | FIA_AFL.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FIA_ATD.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FIA_SOS.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FIA_UAU.2(1) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FIA_UID.2(1) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FIA_USB.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| アクセス制御 | FDP_ACC.1(1) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FDP_ACF.1(1) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FDP_ACC.1(2) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FDP_ACF.1(2) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FRU_RSA.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FTA_MCS.2 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FMT_MTD.1(1) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| 監査 | FAU_GEN.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FAU_GEN.2 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FAU_SAR.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FAU_SAR.2 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FAU_SAR.3 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FAU_STG.1 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FAU_STG.4 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| セキュリティ管理 | FMT_MOF.1 | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_MSA.1 | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_MSA.3(1) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_MSA.3(2) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_MTD.1(2) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_MTD.1(3) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_MTD.1(4) | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FMT_MTD.3 | FPT_RVM.1 | FPT_SEP.1 | FMT_MOF.1 |
| | FMT_SAE.1 | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_SMF.1 | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_SMR.1(1) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FPT_STM.1 | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FPT_RVM.1 | N/A | FPT_SEP.1 | N/A |
| | FPT_SEP.1 | FPT_RVM.1 | N/A | N/A |
| OS に依存する機能 | FMT_SMR.1(2) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FMT_MSA.3(3) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FIA_UAU.2(2) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FIA_UID.2(2) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FDP_ACC.1(3) | FPT_RVM.1 | FPT_SEP.1 | N/A |
| | FDP_ACF.1(3) | FPT_RVM.1 | FPT_SEP.1 | N/A |

各機能が動作する場合、最初にセキュリティ機能が呼び出され、成功した場合にのみ、その動作進行が許可されることによって、迂回を抑止している。また、利用者が処理を行う空間と、TOE が動作する空

間を分離することによって、各種機能への干渉を抑止している。さらに、セキュリティ機能のふるまいの管理を管理者のみに許可することによって、セキュリティ機能が非活性化されることを抑止している。

### 8.2.3. TOE 保証要件根拠

本 ST では、システムインテグレータがシステムの受託開発業務において、本 TOE を利用することを想定している。そのような利用環境において市場は、独立した第三者が、本 TOE が利用者のデータ保護に充分配慮しているといった保証を提供することを望んでいる。市場の求める保証内容は、第三者による TOE の外部インターフェースの識別、独立テストによるセキュリティ機能の確認、提供されるガイダンスの調査などであり、そのような要求を満たす評価保証レベルとしては EAL1 が適している。
また、TOE の導入・運用に際してはシステムインテグレータが TOE を構成要素とするシステム全体に対して品質保証・運用サポートを提供することから、本 TOE 単体の製品保証レベルについては EAL1 で十分であり妥当である。

### 8.2.4. 機能強度根拠

PostgreSQL 認証版は一般のコマーシャルシステムの中で利用されることを想定しているため、想定される不正行為は、公開情報を利用した攻撃である。このため、攻撃者の攻撃力は“低レベル”である。攻撃者は認証を迂回して PostgreSQL 認証版を利用することはできず、低レベルの攻撃能力を持つ攻撃者からの公開情報を利用した不正行為に対抗できるため、PostgreSQL 認証版の最小機能強度レベルは“SOF-基本”である。

## 8.3. TOE 要約仕様根拠

セキュリティ機能要件とセキュリティ仕様概要の対応関係一覧を下表に示す。

**表 8.5 セキュリティ機能要件とセキュリティ仕様概要の対応関係一覧**

| セキュリティ仕様概要 / セキュリティ機能要件 | | F.SEL.PARA | F.USER.DEF | F.USER.AUTHEN | F.USER.PRIV | F.USER.RES | F.USER.REF | F.RES.ATTR | F.AUDIT.COL | F.AUDIT.VIEW | F.AUDIT.SPACE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 認証・識別 | FIA_AFL.1 | | | ✓ | | | | | | | |
| | FIA_ATD.1 | | ✓ | | ✓ | ✓ | | | | | |
| | FIA_SOS.1 | | | ✓ | | | | | | | |
| | FIA_UAU.2(1) | | | ✓ | | | | | | | |
| | FIA_UID.2(1) | | | ✓ | | | | | | | |
| | FIA_USB.1 | | | | ✓ | ✓ | | | | | |
| アクセス制御 | FDP_ACC.1(1) | | | | ✓ | | | | | | |
| | FDP_ACF.1(1) | | | | ✓ | | | | | | |
| | FDP_ACC.1(2) | | | | ✓ | | | | | | |
| | FDP_ACF.1(2) | | | | ✓ | | | | | | |
| | FRU_RSA.1 | | | | | ✓ | | | | | |
| | FTA_MCS.2 | | | | | ✓ | | | | | |
| | FMT_MTD.1(1) | | | | | | | ✓ | | | |
| 監査 | FAU_GEN.1 | | | | | | | | ✓ | | |
| | FAU_GEN.2 | | | | | | | | ✓ | | |
| | FAU_SAR.1 | | | | | | | | | ✓ | |
| | FAU_SAR.2 | | | | | | | | | ✓ | |
| | FAU_SAR.3 | | | | | | | | | ✓ | |
| | FAU_STG.1 | | | | | | | | | | ✓ |
| | FAU_STG.4 | | | | | | | | | | ✓ |
| セキュリティ管理 | FMT_MOF.1 | ✓ | | | ✓ | | | | | | |
| | FMT_MSA.1 | | | ✓ | ✓ | ✓ | | | | | |
| | FMT_MSA.3(1) | | | | ✓ | | | | | | |
| | FMT_MSA.3(2) | | | | ✓ | | | | | | |
| | FMT_MTD.1(2) | ✓ | | | ✓ | | | | | | ✓ |
| | FMT_MTD.1(3) | | ✓ | ✓ | ✓ | | ✓ | | | | |
| | FMT_MTD.1(4) | ✓ | | | ✓ | | | | | ✓ | ✓ |
| | FMT_MTD.3 | ✓ | ✓ | ✓ | ✓ | | | | | | |
| | FMT_SAE.1 | | | ✓ | | | | | | | |
| | FMT_SMF.1 | ✓ | | | ✓ | ✓ | | | | ✓ | ✓ |
| | FMT_SMR.1(1) | | ✓ | | | | | | | | |
| | FPT_STM.1 | | | ✓ | | | | | ✓ | ✓ | |

なお、セキュリティ保証要件については、「表 6.4　保証要件コンポーネント名と保証手段 (p60)」に示すように、すべてのTOEセキュリティ保証要件は保証手段として示されたドキュメントのセットにより対応される。
また、保証手段として示された各ドキュメントにより、本セキュリティターゲットが規定した TOE セキュリティ保証要件が要求する事項を満たしている。

### ■　認証・識別に関するセキュリティ機能要件

認証・識別に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

#### FIA_AFL.1

本セキュリティ機能要件では、利用者の認証における失敗時にその接続を拒否し事象を監査ログとして取得できる必要がある。
セキュリティ機能 F.USER.AUTHEN は認証の失敗時には接続を拒否する。また、認証の成功および失敗事象を監査ログとして取得するので、セキュリティ機能要件を満足している。

#### FIA_ATD.1

本セキュリティ機能要件では、管理者は利用者に対する利用可能範囲を維持できる必要がある。
セキュリティ機能 F.USER.DEF は利用者登録する際に、利用可能範囲を設定できる。
セキュリティ機能 F.USER.PRIV によって、管理者はデータベースにアクセスする権限を利用者に対して付与することができ、セキュリティ機能 F.USER.RES によって各利用者が使用可能な資源量を制限することができる。
これら３つのセキュリティ機能の組み合わせによって、管理者は利用者に対してその利用可能範囲を維持でき、セキュリティ機能要件を満足している。

#### FIA_SOS.1

本セキュリティ機能要件では、利用者が指定する認証情報について、ある程度の複雑さをもたなければならない。
セキュリティ機能 F.USER.AUTHEN は、認証情報（パスワード）に関して TOE が予め定める非類似性品質を満たすこと、または管理者がセキュリティパラメタにより定める最低文字列長（デフォルト:８ 最大:２５５）以上の順列確率的複雑さを要求する。基準が満たされない場合には認証情報の登録を拒否するため、セキュリティ機能要件を満足している。

#### FIA_UAU.2(1)

本セキュリティ機能要件では、TOE の利用前に利用者が識別された利用者本人であることを確認できる必要がある。
セキュリティ機能 F.USER.AUTHEN は、TOE の利用前に識別された利用者の認証情報による確認を行うため、セキュリティ機能要件を満足している。

FIA_UID.2(1)

本セキュリティ機能要件では、TOE の利用前に利用者を識別できる必要がある。
セキュリティ機能 F.USER.AUTHEN は、TOE の利用前に利用者の識別を行うため、セキュリティ機能要件を満足している。

FIA_USB.1

本セキュリティ機能要件では、利用者にその利用者のセキュリティ属性を関連付ける必要がある。
セキュリティ機能 F.USER.PRIV で、利用者は管理者に与えられた権限の範囲で表の操作を行う。
セキュリティ機能 F.USER.RES は、利用者は管理者により制限された資源量の範囲で表の操作を行う。
以上２つのセキュリティ機能により、表の操作時には利用者のセキュリティ属性が関連付けられているため、セキュリティ機能要件を満足している。

■ アクセス制御に関するセキュリティ機能要件

アクセス制御に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

FDP_ACC.1(1)

本セキュリティ機能要件では、管理者は全ての資源に対する全ての操作を実行できる必要がある。
セキュリティ機能 F.USER.PRIV では、バックエンドプロセスは、管理者のプロセスからのデータベースへのアクセス要求に対し、全ての資源に対する全ての操作を実行するので、セキュリティ機能要件を満足している。

FDP_ACF.1(1)

本セキュリティ機能要件では、管理者は全ての資源に対する全ての操作を常に実行できる必要がある。
セキュリティ機能 F.USER.PRIV では、バックエンドプロセスは、管理者のプロセスからのデータベースへのアクセス要求に対し、全ての資源に対する全ての操作を実行するので、セキュリティ機能要件を満足している。

FDP_ACC.1(2)

本セキュリティ機能要件では、利用者は、管理者に付与された権限の範囲内で資源に対する操作を行う必要がある。
セキュリティ機能 F.USER.PRIV では、バックエンドプロセスは、利用者のプロセスからのデータベースへのアクセス要求に対し、その利用者が管理者から付与されたデータベースに対する操作の権限の範囲でのみデータベースに対する操作を行うため、セキュリティ機能要件を満足している。

FDP_ACF.1(2)

本セキュリティ機能要件では、利用者は、管理者に付与された権限の範囲内で資源に対する操作を行う

必要がある。
セキュリティ機能 F.USER.PRIV では、バックエンドプロセスは、利用者のプロセスからのデータベースへのアクセス要求に対し、その利用者が管理者から付与されたデータベースに対する操作の権限の範囲でのみデータベースに対する操作を行うため、セキュリティ機能要件を満足している。

**FRU_RSA.1**
本セキュリティ機能要件では、各利用者が１つのセションで利用可能なメモリ量、ファイル量の制限が行える必要がある。
セキュリティ機能 F.USER.RES は、管理者がセキュリティパラメタに適切な値を指定することで、一人の利用者が１つのセションで利用可能なメモリ量、ファイル量を制限することができ、セキュリティ機能要件を満足している。

**FTA_MCS.2**
本セキュリティ機能要件では、各利用者が同時に利用可能なセション数の制限が行える必要がある。
セキュリティ機能 F.USER.RES は、管理者がセキュリティパラメタに適切な値を指定することで、一人の利用者が同時に利用可能なセション数を制限することができ、セキュリティ機能要件を満足している。

**FMT_MTD.1(1)**
本セキュリティ機能要件では、管理者にのみ TSF データに対する読み出し可能な属性の設定が行われる必要がある。
セキュリティ機能 F.RES.ATTR によって、システムカタログ、ログファイル、作業用ファイルは管理者のみ読み出し可能であり、セキュリティ機能要件を満足している。

### ■ 監査に関するセキュリティ機能要件

監査に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

**FAU_GEN.1**
本セキュリティ機能要件では、監査対象事象について、監査記録を取得可能である必要がある。
セキュリティ機能 F.AUDIT.COL によって、監査記録は本セキュリティ機能要件で定義した情報が常に取得可能であり、セキュリティ機能要件を満足している。

**FAU_GEN.2**
本セキュリティ機能要件では、監査対象事象について、その事象を誰が発生させたか記録する必要がある。
セキュリティ機能 F.AUDIT.COL によって、取得する監査記録には、管理者または利用者名が常に記録されるため、セキュリティ機能要件を満足している。

**FAU_SAR.1**

本セキュリティ機能要件では、管理者のみ監査記録を読み出すことが可能である必要がある。
セキュリティ機能 F.AUDIT.VIEW は、監査記録データベースに対する属性として管理者のみアクセス可としているため、管理者のみ読み出すことができる。さらに、管理者以外のデータベース操作を全て不可能にすることにより管理者の監査記録読み出しの妨害に対抗することもできるため、セキュリティ機能要件を満足している。

**FAU_SAR.2**

本セキュリティ機能要件では、管理者以外の利用者は、読み出しが失敗する必要がある。
セキュリティ機能 F.AUDIT.VIEW は、監査記録データベースに対する属性として管理者のみアクセス可としているため、利用者のアクセスは拒否される。
これによりセキュリティ機能要件を満足している。

**FAU_SAR.3**

本セキュリティ機能要件では、取得した監査記録について、検索、分類、並べ替えして読み出せる必要がある。
セキュリティ機能 F.AUDIT.VIEW は、データベース形式の監査記録に対して、監査記録の参照時には、SQL 文を用いることで、その取り出しおよび整列を行うことを可能としているため、セキュリティ機能要件を満足している。

**FAU_STG.1**

本セキュリティ機能要件では、監査記録が改変、削除されてはならない。
利用者は TSFI を介して監査記録にアクセスすることはできないので改変は行なえない。
セキュリティ機能 F.AUDIT.SPACE では、管理者のみ監査記録の削除を行えるため、監査記録の不当な削除は行えない。
これによりセキュリティ機能要件を満足している。

**FAU_STG.4**

本セキュリティ機能要件では、監査ログが満杯になった場合の振る舞いについて決定し、監査記録の取得を失敗してはならない。
セキュリティ機能 F.AUDIT.SPACE は、監査ログが満杯になった場合、管理者がセキュリティパラメタに設定した内容に従うことによって満杯時の動作を決定し、常に最新の監査ログに関しては損失を防ぐことができ、セキュリティ機能要件を満足している。

### ■ セキュリティ管理に関するセキュリティ機能要件

セキュリティ管理に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

**FMT_MOF.1**

本セキュリティ機能要件では、管理者によってのみ、セキュリティの振る舞いが決定／変更され、また、動作／停止が行われる必要がある。

セキュリティの振る舞いの決定／変更、あるいは動作／停止はセキュリティパラメタの設定により行われる。セキュリティ機能 F.SEL.PARA によって、管理者のみセキュリティパラメタを設定することが可能であり、また、セキュリティパラメタの設定を含むデータの保守は、セキュリティ機能 F.USER.PRIV によって管理者のみ行うことが可能である。

以上２つのセキュリティ機能により、管理者によってのみ、セキュリティの振る舞いが決定／変更され、また、動作／停止が行われるため、セキュリティ機能要件を満足している。

**FMT_MSA.1**

本セキュリティ機能要件では、利用者と利用者が利用可能な資源、それに対する操作や、資源量を管理できるのは管理者のみでなくてはならない。

セキュリティ機能 F.USER.PRIV によって、管理者のみ利用者に対しデータベースに対する操作の権限付与および剥奪を行うことができる。

セキュリティ機能 F.USER.RES によって、管理者のみ利用者が使用可能な資源量を制限できる。

以上２つのセキュリティ機能により、セキュリティ機能要件を満足している。

**FMT_MSA.3(1)**

本セキュリティ機能要件では、管理者が利用可能な資源、それに対する操作の初期値が設定され変更できない必要がある。

セキュリティ機能 F.USER.PRIV によって、管理者に対する初期値として、全ての表に対して全ての操作を行うように設定され、その初期値を変更することはできないため、セキュリティ機能要件を満足している。

**FMT_MSA.3(2)**

本セキュリティ機能要件では、利用者が利用可能な資源、それに対する操作の初期値が設定され変更できない必要がある。

利用者が利用可能な資源、それに対する操作の初期値は、セキュリティ機能 F.USER.PRIV によって、全ての表に対する全ての操作が不可能に設定されており、その初期値を変更することはできないため、セキュリティ機能要件を満足している。

**FMT_MTD.1(2)**

本セキュリティ機能要件では、TSF データの初期値変更、削除が可能なのは管理者のみでなくてはならない。

セキュリティ機能 F.SEL.PARA によって、管理者のみセキュリティパラメタを変更することにより、全利用者共通の使用可能資源量、同時使用セション数の変更が可能である。

セキュリティ機能 F.USER.PRIV によって、管理者のみデータの保守を行うためのコマンドを使用することでログファイルの削除が可能である。
セキュリティ機能 F.AUDIT.SPACE によって、管理者のみ監査記録の削除を行える。
以上３つのセキュリティ機能により、システムカタログ、ログファイルの初期値変更、削除が行えるのは管理者のみであるため、セキュリティ機能要件を満足している。

**FMT_MTD.1(3)**

本セキュリティ機能要件では、利用者毎の TSF データの問い合わせ、改変が可能なのは、管理者および、そのセキュリティ属性に関連付けられた利用者のみでなくてはならない。
セキュリティ機能 F.USER.DEF によって、利用者の登録、変更、および削除を行うことにより、管理者のみ識別情報の変更が行える。
セキュリティ機能 F.USER.PRIV によって、アクセス権限を変更可能なのは管理者のみである。
セキュリティ機能 F.USER.REF によって、管理者は、全利用者の識別認証情報、権限情報、使用可能資源量を、利用者は、自分に関する識別認証情報、権限情報、使用可能資源量のみ参照できる。
セキュリティ機能 F.USER.AUTHEN によって、管理者は、全利用者の認証情報を、利用者は、自分の認証情報を変更できる。
以上４つのセキュリティ機能により、管理者は、全利用者の認証情報、権限情報、セキュリティパラメタ（使用可能資源量など利用者毎にあるもの）の問い合わせ、改変が可能であり、利用者は、自分自身の識別認証情報、権限情報、およびセキュリティパラメタ（使用可能資源量など利用者毎にあるもの）の問い合わせ、改変が可能であるため、セキュリティ機能要件を満足している。

**FMT_MTD.1(4)**

本セキュリティ機能要件では、TSF データの問い合わせ、改変が可能なのは管理者のみでなくてはならない。
セキュリティ機能 F.SEL.PARA によって、管理者のみセキュリティパラメタを変更することが可能である。
セキュリティ機能 F.USER.PRIV によって、セキュリティパラメタにアクセス可能なのは管理者のみである。
セキュリティ機能 F.AUDIT.VIEW は、監査記録データベースに対する属性として管理者のみアクセス可としているため、管理者のみ読み出すことができる。
セキュリティ機能 F.AUDIT.SPACE では、管理者のみ監査記録の削除を行える。
以上４つのセキュリティ機能により、システムカタログ、ログファイルの問い合わせ、改変が可能なのは管理者のみであるため、セキュリティ機能要件を満足している。

**FMT_MTD.3**

本セキュリティ機能要件では、TSF データに対して設定される値はセキュアでなくてはならない。
セキュリティ機能 F.SEL.PARA によって、セキュリティパラメタの値がセキュアな値かどうかチェック

される。
セキュリティ機能 F.USER.DEF によって、識別情報が TOE に登録可能な識別情報かチェックされる。
セキュリティ機能 F.USER.AUTHEN によって、認証情報が使用可能な認証情報かチェックされる。
セキュリティ機能 F.USER.PRIV によって、付与しようとする対象の資源および操作が適切かチェックされる。
以上４つのセキュリティ機能により、セキュリティパラメタ、権限情報、および識別認証情報に対して設定される値はセキュアである。
以上により、TSF データに対して設定される値はセキュアであり、セキュリティ機能要件を満足している。

**FMT_SAE.1**

本セキュリティ機能要件では、管理者は認証情報に有効期限を設けることが可能である必要がある。
セキュリティ機能 F.USER.AUTHEN によって、管理者は、利用者の認証情報に有効期限を設定することができるため、セキュリティ機能要件を満足している。

**FMT_SMF.1**

本セキュリティ機能要件では、「表 5.3　管理要件パラメタ一覧」で与えられる管理項目の管理が行える。
セキュリティ機能 F.SEL.PARA および F.USER.RES によって、管理者のみセキュリティパラメタやセキュリティ属性を変更することが可能である。
同様に、セキュリティ機能 F.USER.PRIV によって、管理者のみセキュリティパラメタの閲覧およびデータの保守を行うことが可能である。監査記録についても、セキュリティ機能 F.AUDIT.VIEW によって、監査記録データベースに対する属性として管理者のみアクセス可としているため、管理者のみ読み出すことができ、セキュリティ機能 F.AUDIT.SPACE によって、管理者のみ監査記録の削除を行える。
以上５つのセキュリティ機能により、「表 5.3　管理要件パラメタ一覧」で与えられる管理項目の管理が行えるため、セキュリティ機能要件を満足している。

**FMT_SMR.1(1)**

本セキュリティ機能要件では、管理者、利用者という役割が維持される必要がある。
セキュリティ機能 F.USER.DEF によって、管理者は管理者として登録され、利用者は管理者により利用者として登録されるため、セキュリティ機能要件を満足している。

**FPT_STM.1**

本セキュリティ機能要件では、高信頼タイムスタンプを提供できなければならない。
セキュリティ機能 F.AUDIT.COL において監査ログは高信頼タイムスタンプを用いて記録される。セキュリティ機能 F.AUDIT.VIEW によって、管理者は高信頼タイムスタンプを用いて監査記録を検索・参照できる。また、セキュリティ機能 F.USER.AUTHEN において、管理者は高信頼タイムスタンプを用いて認証情報の有効期限を定義することができる。

以上３つのセキュリティ機能において、高信頼タイムスタンプは一貫して利用されているため、セキュリティ機能要件を満足している。

### 8.3.1. 機能強度仕様根拠

TOE は、F.USER.AUTHEN として利用者に対する識別認証を行っている。
認証情報が従う品質基準として、以下の確率的または順列的メカニズムを採用している。

- 以下の文字で構成される文字列定数で指定
  英字
  数字
  以下の特殊文字
  , ( ) . : ; = * + - / ? < > % _ ’ ”
  以下の拡張文字
  @ ￥ #
- パスワードはセキュリティパラメタで指定されるパスワードの最低長（デフォルト:８ 最大値:２５５）以上であり、かつパスワードを構成する文字を４つのクラス（数字、大文字の英字、小文字の英字、それ以外）に分類した際に、それぞれのクラスの文字を含まなければならない。
- あるいは、構成する文字のクラス数が４より小さい場合は、パスワード長はクラス数が少ない分、最低長よりも長くなければならない。
- パスワードを変更する際には、大文字と小文字を同一の文字とみなして新旧を比較した場合、両者が同一、一方が他方を反転したもの、一方が他方を包含するものであってはならない。

F.USER.AUTHEN では、不成功認証の際に、その利用者と事象発生時刻を監査ログとして取得する。

これらにより、F.USER.AUTHEN の強度は中レベルの攻撃能力を持つ攻撃者に対して十分に対抗することができるため、SOF-中位が妥当であると判断する。これは、IT セキュリティ要件で主張した最小機能強度 SOF-基本を満足し、特定の TOE セキュリティ機能要件（対象は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2(1)、FIA_UID.2(1)）に対する機能強度 SOF-中位と一貫するものである。

## 8.4. PP 主張根拠

PP 準拠なし。

# 【用語】

**アプリケーション**

本書では、利用者が作成するアプリケーションプログラムすべてを指す。

**エレメント**

本書では、監査ログエレメントを指す。監査ログは監査記録を複数個の単位に分割して格納する。この分割の単位を監査ログエレメント(または略してエレメント)と呼ぶ。

**監査ログ**

日常の管理者および利用者の監視や、セキュリティ上の問題が発生した場合の原因を特定するための情報として、利用者の行った処理、管理者の行った処理、発生した異常な事象をログとして残している。このログを監査ログと呼ぶ。

**管理者**

本書では、PostgreSQL 認証版を管理する管理者を指す。また、PostgreSQL 認証版の管理者は OS の管理者でもある。

**コマンド**

本書では、PostgreSQL 認証版を運用するためのコマンドを指す。

**共用メモリ**

プロセス間で相互に参照が可能なメモリ領域をいう。

**バックエンドプロセス**

本書では、アプリケーションやコマンドの処理を行う PostgreSQL 認証版のプロセスを指す。

**作業用ファイル**

作業用テーブルおよび作業用ソート領域を指す。

**シーケンス**

一意性のある番号を順番に取得する機能

例)　１から順に値を取得するシーケンスを事前に定義する

順序　：　１から順番に昇順に値を採番

以下の SQL 文を繰り返し実行すると、表の列に１から順番に値が入る。

INSERT INTO 表　VALUES 列 = 順序.NEXTVAL;

**スーパユーザ**

UNIX（Linux を含む）システムを管理する特別の権限を持ったシステム管理者のことを指す。

**責任者**

本書では、セキュリティシステムの全責任を担う責任者を指す。責任者は、ふさわしい管理者の選任、管理者の教育等を行う必要がある。

**セキュリティパラメタ**

セキュリティシステムにおいて、PostgreSQL 認証版のアクセスを制約する各種パラメタを指す。

**セション**

PostgreSQL 認証版に結合した時点から結合解除までの間を指す。

**データベース**

相互に関連するデータを整理・統合し，検索しやすくしたファイル。また，このようなファイルの共用を可能にするシステム。

**データベーススペース**

利用者のデータが格納されているファイル。データベーススペースには、論理的なアクセスの単位である表が格納されており、利用者のデータは、この表に格納される。

**システムカタログ**

利用者が利用するデータベースに対して、データベースの論理構造／格納構造／物理構造に関する情報が格納されている。

**動作環境ファイル**

アプリケーションの実行時の動作環境を規定するためのファイル。

**ファイル**

本書では、ファイルシステム上のファイルを指す。

**関数**

SQL 記述性を高めるために、複雑な演算処理をあらかじめデータベースに登録する機能である。

例） 二つの値の平均をとる関数を事前に定義

HEIKIN ： 復帰値 = （入力１ ＋ 入力２）/ ２

以下の SQL 文で結果表を参照すると、二つのカラム結果１と結果２の平均が取得できる。

SELECT HEIKIN(結果 1,結果 2) FROM 結果表;

**プロセス**

UNIX（Linux を含む）システムの仕事の単位を指す。

**利用者**

本書では、PostgreSQL 認証版を利用する一般利用者を指す。

**リレーショナルデータベース**

PostgreSQL 認証版が採用しているデータベースである。リレーショナルデータベースでは、データを行と列からなる二次元の表で表現する。データベース操作は、データベース言語 SQL で行う。

**ALTER ROLE 文**

利用者変更文。利用者の属性を変更する DDL 文。

**CREATE ROLE 文**

利用者定義文。データベースシステムにアクセスする利用者を定義する DDL 文。

**DDL 文**

データ定義文。データベースの作成、削除等に使用する SQL 文。

**DELETE 権**

表の行を削除するための権限。

**DML 文**

データ操作文。データベースの参照、追加、削除および更新に使用する SQL 文。

**DROP ROLE 文**

利用者削除文。利用者の定義を削除する DDL 文。

**EXECUTE 権**

関数を実行するための権限。

**GRANT 文**

利用者に対して権限を付与する DDL 文。

**INSERT 権**

表に行を挿入するための権限。

**RDB**

Relational DataBase の省略形。リレーショナルデータベースに同じ。

**REVOKE 文**

利用者に対して付与した権限を剥奪する DDL 文。

**SELECT 権**

表の行を参照するための権限。

**SET 文**

セキュリティパラメタを設定するための DDL 文。

**SQL**

国際標準のリレーショナルデータベース操作言語であり、データベースの構造を定義するＤＤＬ(Data Definition Language)とデータベースへのデータの入力、登録、更新、変更、削除、検索などの操作を行うＤＭＬ(Data Manipulation Language)より構成される。

**TCP/IP**

Transmission Control Protocol/Internet Protocol の省略形。データ通信を行うため、信号送信の手順、データの表現法、誤り検出法などを定める通信規約（通信プロトコル）のひとつ。インターネットの標準プロトコルとして、現在最も普及しているプロトコル。

**UPDATE 権**

表の行を更新するための権限。

# 【略語】

**CC** コモンクライテリア(Common Criteria)

**EAL** 評価保証レベル（Evaluation Assurance Level ）

**IT** 情報技術（Information Technology ）

**PP** プロテクションプロファイル（Protection Profile ）

**SF** セキュリティ機能（Security Function ）

**SFP** セキュリティ機能方針（Security Function Policy ）

**SOF** 機能強度（Strength of Function ）

**ST** セキュリティターゲット（Security Target ）

**TOE** 評価対象（Target of Evaluation ）

**TSC** TSF 制御範囲（TSF Scope of Control ）

**TSF** TOE セキュリティ機能（TOE Security Functions ）

**TSFI** TSF インターフェース（TSF Interface ）

**TSP** TOE セキュリティ方針（TOE Security Policy ）

# 見出し一覧